CYBER SECURITY

POUR MAC

Guide de l'utilisateur

(version 6.0 et ultérieures)

Cliquez ici pour télécharger la version la plus récente de ce document

© **ESET, spol. s r.o.**
ESET Cyber Security a été développé par ESET, spol. s r.o.
Pour plus d'informations, visitez www.eset.com.
Tous droits réservés. Aucune partie de cette documentation ne peut être reproduite, stockée dans un système d'archivage ou transmise sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement, numérisation ou autre, sans l'autorisation écrite de l'auteur.
ESET, spol. s r.o. se réserve le droit de modifier les applications décrites sans préavis.

Service client : www.eset.com/support

REV. 1. 10. 2015

Sommaire

1. ESET Cyber Security 4
1.1 Nouveautés de la version 6 4
1.2 Configuration système 4
2. Installation 4
2.1 Installation standard 4
2.2 Installation personnalisée 5
3. Activation de produit 5
4. Désinstallation 6
5. Brève présentation 6
5.1 Raccourcis clavier 6
5.2 Vérification de l'état de la protection 6
5.3 Que faire lorsque le programme ne fonctionne pas correctement ? 6
6. Protection de l'ordinateur 6
6.1 Protection antivirus et antispyware 7
6.1.1 Général 7
6.1.1.1 Exclusions 7
6.1.2 Protection au démarrage 7
6.1.3 Protection en temps réel du système de fichiers 7
6.1.3.1 Moment de l'analyse (analyse déclenchée par un événement) 8
6.1.3.2 Options avancées 8
6.1.3.3 Quand faut-il modifier la configuration de la protection en temps réel ? 8
6.1.3.4 Vérification de la protection en temps réel 8
6.1.3.5 Que faire si la protection en temps réel ne fonctionne pas ? 8
6.1.4 Analyse de l'ordinateur à la demande 9
6.1.4.1 Type d'analyse 9
6.1.4.1.1 Analyse intelligente 9
6.1.4.1.2 Analyse personnalisée 9
6.1.4.2 Cibles à analyser 9
6.1.4.3 Profils d'analyse 9
6.1.5 Configuration des paramètres du moteur ThreatSense 10
6.1.5.1 Objets 10
6.1.5.2 Options 11
6.1.5.3 Nettoyage 11
6.1.5.4 Exclusions 11
6.1.5.5 Limites 11
6.1.5.6 Autres 11
6.1.6 Une infiltration est détectée 12
6.2 Analyse et blocage de supports amovibles 12
7. Antihameçonnage 12
8. Protection Internet et de la messagerie 13
8.1 Protection Web 13
8.1.1 Ports 13
8.1.2 Mode actif 13
8.1.3 Listes d'URL 13
8.2 Protection de la messagerie 13
8.2.1 Vérification par protocole POP3 14
8.2.2 Vérification par protocole IMAP 14
9. Mettre à jour 14
9.1 Configuration des mises à jour 14
9.1.1 Configuration avancée 14
9.2 Comment créer des tâches de mise à jour 15
9.3 Mise à jour de ESET Cyber Security vers une nouvelle version 15
9.4 Mises à jour du système 15
10. Outils 15
10.1 Fichiers journaux 16
10.1.1 Maintenance des journaux 16
10.1.2 Filtrage des journaux 16
10.2 Planificateur 16
10.2.1 Création de nouvelles tâches 17
10.2.2 Création de tâches définies par l'utilisateur 17
10.3 Quarantaine 17
10.3.1 Mise en quarantaine de fichiers 18
10.3.2 Restauration depuis la quarantaine 18
10.3.3 Soumission de fichiers de quarantaine 18
10.4 Processus en cours 18
10.5 Live Grid 18
10.5.1 Configuration de Live Grid 19
10.6 ESET Social Media Scanner 19
11. Interface utilisateur 19
11.1 Alertes et notifications 19
11.1.1 Configuration avancée des alertes et notifications 20
11.2 Privilèges 20
11.3 Menu contextuel 20
12. Divers 20
12.1 Importer et exporter les paramètres 20
12.1.1 Importer les paramètres 20
12.1.2 Exporter les paramètres 20
12.2 Configuration du serveur proxy 20
13. Glossaire 21
13.1 Types d'infiltrations 21
13.1.1 Virus 21
13.1.2 Vers 21
13.1.3 Chevaux de Troie 21
13.1.4 Rootkits 21
13.1.5 Logiciels publicitaires 21
13.1.6 Spyware 22
13.1.7 Applications potentiellement dangereuses 22
13.1.8 Applications potentiellement indésirables 22
13.2 Types d'attaques à distance 22
13.2.1 Attaques par déni de service 22
13.2.2 Empoisonnement du cache DNS 22
13.2.3 Balayage de ports 23
13.2.4 Désynchronisation TCP 23
13.2.5 Relais SMB 23
13.2.6 Attaques par ICMP 23
13.3 Courrier électronique 23
13.3.1 Publicités 24
13.3.2 Canulars 24
13.3.3 Hameçonnage 24
13.3.4 Identification du spam 24

1. ESET Cyber Security

ESET Cyber Security représente une nouvelle approche d'une sécurité véritablement intégrée de l'ordinateur. La version la plus récente du moteur d'analyse ThreatSense® combine rapidité et précision pour sécuriser votre ordinateur. Cette combinaison produit un système intelligent qui protège constamment votre ordinateur des attaques et des logiciels malveillants.

ESET Cyber Security est une solution complète de sécurité qui résulte de notre engagement à long terme d'offrir à la fois une protection maximale et un impact minimal sur le système. Les technologies avancées de ESET Cyber Security, basées sur l'intelligence artificielle, permettent une élimination proactive des infiltrations de virus, vers, chevaux de Troie, spyware, logiciels publicitaires, rootkits et autres attaques basées sur Internet sans handicaper les performances du système.

1.1 Nouveautés de la version 6

Par rapport à la version 5 d'ESET Cyber Security, la version 6 comprend les mises à jour et améliorations suivantes :

Antihameçonnage
Empêche les faux sites Web dont l'apparence est identique à celle de sites Web fiables de récupérer vos informations personnelles.

Intégration d'ESET Social Media Scanner
ESET Cyber Security est lié à une application pour réseaux sociaux conçue pour protéger les comptes Twitter des menaces. Cette application est indépendante des autres produits et est entièrement gratuite.

Mises à jour du système
ESET Cyber Security version 6 comprend différents correctifs et améliorations, notamment des notifications concernant les mises à jour du système d'exploitation. Pour en savoir plus, consultez la section Mises à jour du système 15.

1.2 Configuration système

Pour garantir des performances optimales avec ESET Cyber Security, le système doit au moins répondre à la configuration suivante :

	Configuration système
Architecture du processeur	Intel® 32 bits, 64 bits
Système d'exploitation	Mac OS X version 10.6 et ultérieure
Mémoire	300 Mo
Espace disque disponible	200 Mo

2. Installation

Avant de commencer l'installation, fermez tous les programmes ouverts sur votre ordinateur. ESET Cyber Security contient des composants qui peuvent entrer en conflit avec les autres programmes antivirus qui sont peut-être installés sur votre ordinateur. ESET recommande vivement de supprimer les autres programmes antivirus afin d'éviter tout problème éventuel.

Pour lancer l'assistant d'installation, effectuez l'une des opérations suivantes :

- Si vous effectuez l'installation à partir du CD/DVD d'installation, installez-le dans le lecteur, ouvrez-le à partir du Bureau ou depuis le **Finder**, puis double-cliquez sur l'icône **Installer**.
- Si vous effectuez l'installation depuis un fichier que vous avez téléchargé du site ESET, ouvrez ce fichier et double-cliquez sur l'icône **Installer**.

L'assistant d'installation vous accompagne pendant le processus. Pendant la première phase de l'installation, le programme d'installation recherchera automatiquement la dernière version du produit en ligne. S'il détecte une version plus récente, vous pourrez télécharger la dernière version avant de poursuivre l'installation.

Après avoir accepté les termes du contrat de licence de l'utilisateur final, vous devrez choisir l'un des modes d'installation suivants :

- Installation standard 4
- Installation personnalisée 5

2.1 Installation standard

Le mode d'installation standard comprend des options de configuration qui correspondent à la plupart des utilisateurs. Ces paramètres offrent une sécurité maximale tout en permettant de conserver d'excellentes performances système. L'installation standard est l'option par défaut qui est recommandée si vous n'avez pas d'exigence particulière pour certains paramètres.

Live Grid
Le système d'alerte anticipé Live Grid veille à ce qu'ESET soit immédiatement et continuellement informé des nouvelles infiltrations afin de protéger rapidement nos clients. Ce système permet de soumettre de nouvelles menaces au laboratoire d'ESET, où elles sont analysées, traitées et ajoutées à la base des signatures de virus. L'option **Activer ESET Live Grid (recommandé)** est sélectionnée par défaut. Cliquez sur **Configuration...** pour modifier les paramètres détaillés de soumission des fichiers suspects. Pour plus d'informations, reportez-vous à la section Live Grid 18.

Applications potentiellement indésirables
La dernière étape de l'installation consiste à configurer la détection des **applications potentiellement indésirables**. De tels programmes ne sont pas nécessairement malveillants,

mais peuvent avoir une incidence négative sur le comportement du système d'exploitation. Ces applications sont souvent associées à d'autres programmes et peuvent être difficiles à remarquer lors de l'installation. Ces applications affichent habituellement une notification pendant l'installation, mais elles peuvent facilement s'installer sans votre consentement.

Après l'installation de ESET Cyber Security, vous devez effectuer une analyse de l'ordinateur afin de rechercher tout code malveillant éventuel. Dans la fenêtre principale du programme, cliquez sur **Analyse de l'ordinateur**, puis sur **Analyse intelligente**. Pour plus d'informations sur l'analyse de l'ordinateur à la demande, reportez-vous à la section Analyse de l'ordinateur à la demande 9.

2.2 Installation personnalisée

Le mode d'installation personnalisée est destiné aux utilisateurs expérimentés qui souhaitent modifier les paramètres avancés pendant l'installation.

Serveur proxy
Si vous utilisez un serveur proxy, vous pouvez définir ses paramètres en sélectionnant l'option **J'utilise un serveur proxy**. Dans la fenêtre suivante, entrez l'adresse IP ou l'adresse URL de votre serveur proxy dans le champ **Adresse**. Dans le champ Port, spécifiez le port sur lequel le serveur proxy accepte les connexions (3128 par défaut). Si le serveur proxy exige une authentification, saisissez un **nom d'utilisateur** et un **mot de passe** pour accorder l'accès au serveur proxy. Si vous n'utilisez pas de serveur proxy, sélectionnez l'option **Je n'utilise pas de serveur proxy**. Si vous ne savez pas si vous utilisez un serveur proxy ou non, vous pouvez utiliser vos paramètres système en cours en sélectionnant l'option **Utiliser les paramètres système (recommandée)**.

Privilèges
Dans l'étape suivante, vous pouvez définir les utilisateurs ou groupes privilégiés qui pourront modifier la configuration du programme. Dans la liste des utilisateurs figurant à gauche, sélectionnez les utilisateurs et l'option **Ajouter** pour les ajouter à la liste **Utilisateurs privilégiés**. Pour afficher tous les utilisateurs du système, sélectionnez **Afficher tous les utilisateurs**. Si la liste Utilisateurs privilégiés est vide, tous les utilisateurs sont considérés comme étant privilégiés.

Live Grid
Le système d'alerte anticipé Live Grid veille à ce qu'ESET soit immédiatement et continuellement informé des nouvelles infiltrations afin de protéger rapidement nos clients. Ce système permet de soumettre de nouvelles menaces au laboratoire d'ESET, où elles sont analysées, traitées et ajoutées à la base des signatures de virus. L'option **Activer ESET Live Grid (recommandé)** est sélectionnée par défaut. Cliquez sur **Configuration...** pour modifier les paramètres détaillés de soumission des fichiers suspects. Pour plus d'informations, reportez-vous à la section Live Grid 18.

Applications potentiellement indésirables
L'étape suivante de l'installation consiste à configurer la détection des **applications potentiellement indésirables**. De tels programmes ne sont pas nécessairement malveillants, mais peuvent avoir une incidence négative sur le comportement du système d'exploitation. Ces applications sont souvent associées à d'autres programmes et peuvent être difficiles à remarquer lors de l'installation. Ces applications affichent habituellement une notification pendant l'installation, mais elles peuvent facilement s'installer sans votre consentement.

Après l'installation de ESET Cyber Security, vous devez effectuer une analyse de l'ordinateur afin de rechercher tout code malveillant éventuel. Dans la fenêtre principale du programme, cliquez sur **Analyse de l'ordinateur**, puis sur **Analyse intelligente**. Pour plus d'informations sur l'analyse de l'ordinateur à la demande, reportez-vous à la section Analyse de l'ordinateur à la demande 9.

3. Activation de produit

Après l'installation, la fenêtre Activation du produit s'affiche automatiquement. Pour accéder à tout moment à la boîte de dialogue d'activation du produit, cliquez sur l'icône ESET Cyber Security dans la barre de menus (en haut de l'écran), puis sur **Activation du produit...**.

- **Clé de licence** : chaîne unique au format XXXX-XXXX-XXXX-XXXX-XXXX ou XXXX-XXXXXXXX qui sert à identifier le propriétaire de la licence et à activer cette dernière. Si vous avez acheté une version boîte du produit, activez votre produit à l'aide d'une **clé de licence**. Elle se trouve généralement à l'intérieur du coffret ou au dos de celui-ci.
- **Nom d'utilisateur et mot de passe** : si vous disposez d'un nom d'utilisateur et d'un mot de passe et si vous ne savez pas comment activer ESET Cyber Security, cliquez sur **Je dispose d'un nom d'utilisateur et d'un mot de passe. Que dois-je faire ?**. Vous êtes alors redirigé vers ESET License Administrator où vous pouvez convertir vos informations d'identification en clé de licence.
- **Licence d'essai gratuite** : si vous souhaitez évaluer ESET Cyber Security avant de l'acheter, sélectionnez l'option **Licence d'essai gratuite**. Indiquez votre adresse électronique pour activer ESET Cyber Security pendant un laps de temps limité. La licence d'essai vous sera envoyée par courrier électronique. Les licences d'essai ne peuvent être activées qu'une seule fois par client.
- **Acheter une licence** : si vous n'avez pas de licence et souhaitez en acheter une, cliquez sur **Acheter une licence**. Cette opération vous redirigera vers le site Web de votre distributeur ESET local.
- **Activer ultérieurement** : si vous choisissez de ne pas effectuer l'activation maintenant, cliquez sur **Activer ultérieurement**.

4. Désinstallation

Pour désinstaller ESET Cyber Security, effectuez l'une des opérations suivantes :

- insérez le CD/DVD d'installation ESET Cyber Security dans votre ordinateur, ouvrez-le à partir du Bureau ou de la fenêtre **Finder**, puis double-cliquez sur **Désinstaller**,
- ouvrez le fichier d'installation de ESET Cyber Security (*.dmg*) et double-cliquez sur **Désinstaller**,
- lancez le **Finder**, ouvrez le dossier **Applications** sur le disque dur, appuyez sur CTRL et cliquez sur l'icône **ESET Cyber Security**, puis sélectionnez l'option d'**affichage du contenu du paquet**. Ouvrez le dossier **Contents** > **Helpers**, puis double-cliquez sur l'icône **Uninstaller**.

5. Brève présentation

La fenêtre principale de ESET Cyber Security est divisée en deux sections principales. La fenêtre principale de droite affiche les informations correspondant à l'option sélectionnée dans le menu principal à gauche.

Les sections suivantes sont accessibles à partir du menu principal :

- **Accueil** : fournit des informations sur l'état de protection de votre ordinateur, d'Internet et de la messagerie.
- **Analyse de l'ordinateur** : cette section permet de configurer et de lancer l'analyse de l'ordinateur à la demande 9.
- **Mettre à jour** : affiche des informations sur les mises à jour de la base de signatures de virus.
- **Configuration** : sélectionnez cette section pour ajuster le niveau de sécurité de votre ordinateur.
- **Outils** : permet d'accéder aux fichiers journaux 16, au planificateur 16, à la quarantaine 17, aux processus en cours 18 et à d'autres fonctions du programme.
- **Aide** : permet d'accéder aux fichiers d'aide, à la base de connaissances sur Internet, au formulaire de demande d'assistance et à d'autres informations sur le programme.

5.1 Raccourcis clavier

Raccourcis clavier disponibles avec ESET Cyber Security :

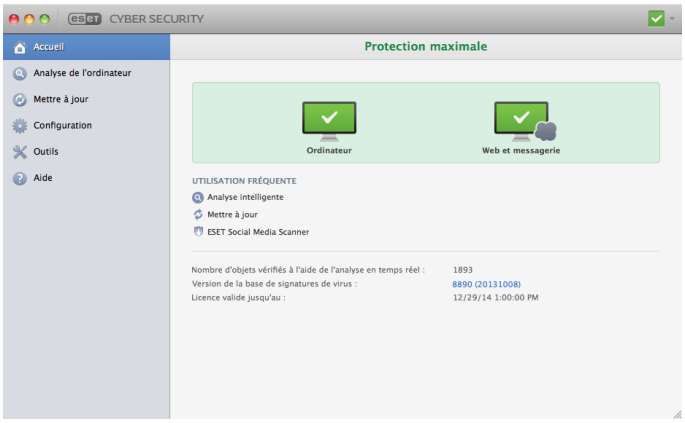
- *cmd+,* : affiche les préférences d'ESET Cyber Security,
- *cmd+U* : ouvre la fenêtre **Configuration du nom d'utilisateur et du mot de passe**,
- *cmd+O* : redimensionne la fenêtre de l'interface utilisateur graphique principale d'ESET Cyber Security pour lui redonner sa taille par défaut et la place au centre de l'écran.

Les raccourcis clavier suivants ne fonctionnent que si l'option **Utiliser le menu standard** est activée dans **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd+,* > **Interface** :

- *cmd+alt+L* : ouvre la fenêtre **Fichiers journaux** ;
- *cmd+alt+S* : ouvre la fenêtre **Planificateur** ;
- *cmd+alt+Q* : ouvre la fenêtre **Quarantaine**.

5.2 Vérification de l'état de la protection

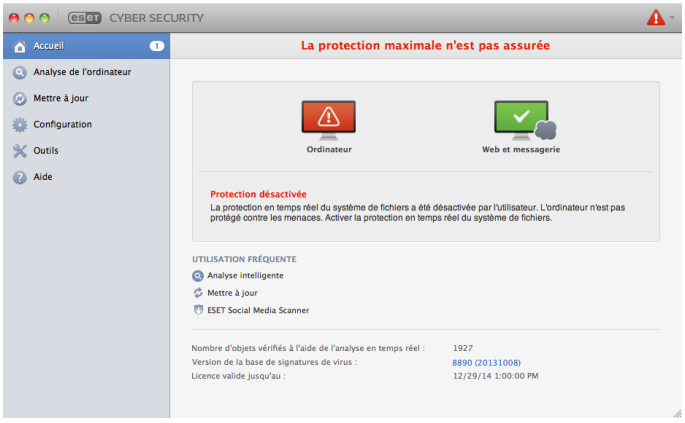
Pour afficher l'état de la protection, cliquez sur **Accueil** dans le menu principal. La fenêtre principale affiche un résumé de l'état de fonctionnement des modules de ESET Cyber Security.



5.3 Que faire lorsque le programme ne fonctionne pas correctement ?

Lorsqu'un module fonctionne correctement, une icône verte s'affiche. Dans le cas contraire, un point d'exclamation rouge ou une icône de notification orange apparaît. Des informations supplémentaires sur le module et une suggestion de solution du problème sont alors présentées. Pour changer l'état des différents modules, cliquez sur le lien bleu affiché sous chaque message de notification.

Si vous ne parvenez pas à résoudre le problème à l'aide des solutions suggérées, vous pouvez chercher une autre solution dans la base de connaissances ESET ou contacter le Service client ESET. Ce dernier répondra rapidement à vos questions et vous aidera à trouver une solution.


CYBER SECURITY
Accueil
Analyse de l'ordinateur
Mettre à jour
Configuration
Outils
Aide
La protection maximale n'est pas assurée
Ordinateur
Web et messagerie
Protection désactivée
La protection en temps réel du système de fichiers a été désactivée par l'utilisateur. L'ordinateur n'est pas protégé contre les menaces. Activer la protection en temps réel du système de fichiers.
UTILISATION FRÉQUENTE
Analyse intelligente
Mettre à jour
ESET Social Media Scanner
Nombre d'objets vérifiés à l'aide de l'analyse en temps réel : 1927
Version de la base de signatures de virus : 8890 (20131008)
Licence valide jusqu'au : 12/29/14 1:00:00 PM

6. Protection de l'ordinateur

La configuration de l'ordinateur se trouve sous **Configuration** > **Ordinateur**. Elle affiche l'état de la **protection en temps réel du système de fichiers** et du **blocage des supports amovibles**. Pour désactiver des modules individuels, réglez le bouton du module en question sur **DÉSACTIVÉ**. Notez que cela peut réduire le niveau de protection de votre ordinateur. Pour accéder aux paramètres détaillés de chaque module, cliquez sur **Configuration...**.

6.1 Protection antivirus et antispyware

La protection antivirus protège des attaques contre le système en modifiant les fichiers représentant des menaces potentielles. Si une menace comportant du code malveillant est détectée, le module Antivirus peut l'éliminer en la bloquant. Il peut ensuite la nettoyer, la supprimer ou la placer en quarantaine.

6.1.1 Général

Dans la section **Général** (**Configuration** > **Saisie des préférences de l'application...** > **Général**), vous pouvez activer la détection des types d'applications suivants :

- **Applications potentiellement indésirables** : ces applications ne sont pas nécessairement malveillantes, mais elles peuvent avoir une incidence négative sur les performances de votre ordinateur. L'installation de ces applications nécessite généralement l'accord de l'utilisateur. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état antérieur à l'installation de ces applications). Les changements les plus significatifs concernent l'affichage indésirable de fenêtres contextuelles, l'activation et l'exécution de processus cachés, l'augmentation de l'utilisation des ressources système, les changements dans les résultats de recherche et les applications communiquant avec des serveurs distants.
- **Applications potentiellement dangereuses** : cette appellation fait référence à des logiciels commerciaux légitimes qui peuvent être mis à profit par des pirates, s'ils ont été installés à l'insu de l'utilisateur. Cette classification inclut des programmes tels que des outils d'accès à distance. Pour cette raison, cette option est désactivée par défaut.
- **Applications suspectes** : ces applications comprennent les programmes compressés à l'aide d'empaqueteurs ou de protecteurs. Ces types de protecteurs sont souvent exploités par les auteurs de logiciels malveillants, afin d'échapper à la détection. Un empaqueteur est un programme exécutable compressé auto-extractible qui regroupe plusieurs sortes de logiciels malveillants dans une seule archive. Les empaqueteurs les plus courants sont au format UPX, PE_Compact, PKLite ou ASPack. Un même logiciel malveillant peut être détecté différemment suivant l'empaqueteur dans lequel il est compressé. Les empaqueteurs ont également la possiblité de modifier leur « signature » au fil du temps, rendant ainsi le logiciel malveillant plus difficile à détecter et à supprimer.

Pour configurer le système de fichiers ou les exclusions Web et messagerie 7, cliquez sur le bouton **Configuration...**.

6.1.1.1 Exclusions

Dans la section **Exclusions**, vous pouvez exclure de l'analyse certains fichiers/dossiers, applications ou adresses IP/IPv6.

Les fichiers et les dossiers répertoriés dans l'onglet **Système de fichiers** seront exclus de tous les analyseurs : au démarrage, en temps réel et à la demande (analyse de l'ordinateur).

- **Chemin** : chemin d'accès aux fichiers et dossiers exclus.
- **Menace** : si le nom d'une menace figure en regard d'un fichier exclu, cela signifie que ce fichier n'est exclu que pour cette menace spécifique : il n'est pas exclu complètement. Si le fichier est infecté ultérieurement par un autre logiciel malveillant, il est détecté par le module antivirus.
- : crée une exclusion. Saisissez le chemin d'accès à l'objet (vous pouvez également utiliser les caractères génériques * et ?) ou sélectionnez le dossier ou le fichier dans la structure arborescente.
- : supprime les entrées sélectionnées.
- **Par défaut** : annule toutes les exclusions.

Dans l'onglet **Web et messagerie**, il est possible d'exclure certaines **applications** ou **adresses IP/IPv6** de l'analyse des protocoles.

6.1.2 Protection au démarrage

La vérification des fichiers de démarrage analyse automatiquement les fichiers lors du démarrage du système. Par défaut, cette analyse s'exécute régulièrement à intervalles planifiés, après la connexion d'un utilisateur ou une mise à jour de la base de signatures de virus. Pour modifier les réglages des paramètres du moteur ThreatSense applicables à l'analyse au démarrage, cliquez sur le bouton **Configuration...**. Vous trouverez dans cette section 10 des informations complémentaires sur la configuration du moteur ThreatSense.

6.1.3 Protection en temps réel du système de fichiers

La protection en temps réel du système de fichiers vérifie tous les types de supports et déclenche une analyse en fonction de différents événements. La protection en temps réel du système de fichiers utilise la technologie ThreatSense (décrite dans la section intitulée Configuration des paramètres du moteur ThreatSense 10) et peut être différente pour les nouveaux fichiers et les fichiers existants. Pour les nouveaux fichiers, il est possible d'appliquer un niveau de contrôle plus approfondi.

Par défaut, la protection en temps réel est lancée au démarrage du système d'exploitation, assurant ainsi une analyse sans interruption. Dans certains cas (par exemple, en cas de conflit avec un autre analyseur en temps réel), il est possible de mettre fin à la protection en temps réel en cliquant sur l'icône ESET Cyber Security dans la barre de menus (en haut de l'écran), puis en sélectionnant l'option **Désactiver la protection en temps réel du système de fichiers**. Il est également possible de désactiver la protection en temps réel du système de fichiers depuis la fenêtre principale du programme (sélectionnez **Configuration** > **Ordinateur** et réglez **Protection en temps réel du système de fichiers** sur **DÉSACTIVÉ**).

Pour modifier les paramètres avancés de la protection en temps réel du système de fichiers, sélectionnez **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd+,*) > **Protection en temps réel** et cliquez sur l'option **Configuration...** située en regard de l'option **Options avancées** (reportez-vous à la section Options d'analyse avancées 8).

6.1.3.1 Moment de l'analyse (analyse déclenchée par un événement)

Par défaut, tous les fichiers sont analysés à l'ouverture, à la création ou à l'exécution. Il est recommandé de conserver les paramètres par défaut, car ils offrent le niveau maximal de protection en temps réel pour votre ordinateur.

6.1.3.2 Options avancées

Vous pouvez définir dans cette fenêtre les types d'objet que le moteur ThreatSense doit analyser, activer/désactiver l'option **Heuristique avancée** et modifier les paramètres des archives et du cache de fichiers.

Il n'est pas recommandé de modifier les valeurs par défaut de la section **Paramètres d'archive par défaut**, à moins que cela ne soit nécessaire pour résoudre un problème spécifique, car l'augmentation des valeurs d'imbrication des archives peut avoir une incidence sur les performances.

Vous pouvez activer ou désactiver l'analyse heuristique avancée ThreatSense de chacun des fichiers exécutés, créés et modifiés en cochant la case **Heuristique avancée** de chaque section de paramètres de ThreatSense.

Pour réduire l'impact de la protection en temps réel sur le système, vous pouvez définir la taille du cache d'optimisation. L'option **Activer le cache des fichiers nettoyés** doit être activée pour que ce paramètre soit pris en compte. Si l'option **Activer le cache des fichiers nettoyés** est désactivée, tous les fichiers sont analysés lorsqu'ils font l'objet d'un accès. Les fichiers ne sont analysés qu'une seule fois après leur mise en cache (sauf s'ils ont été modifiés), jusqu'à ce que le cache soit plein. Les fichiers sont immédiatement réanalysés après chaque mise à jour de la base de signatures de virus. Cliquez sur **Activer le cache des fichiers non infectés** pour activer/désactiver cette fonction. Pour définir la quantité de fichiers à mettre en cache, il vous suffit d'entrer la valeur souhaitée dans le champ de saisie situé en regard de l'option **Taille du cache**.

D'autres paramètres d'analyse peuvent être définis dans la fenêtre **Configuration du moteur ThreatSense**. Vous pouvez définir, pour la protection en temps réel du système de fichiers, le type des **objets** à analyser, les **options** à utiliser et le niveau de **nettoyage**, les **extensions** et les **limites** de taille de fichiers. Vous pouvez ouvrir la fenêtre de configuration du moteur ThreatSense en cliquant sur **Configuration** en regard de l'option **Moteur ThreatSense** dans la fenêtre Configuration avancée. Pour plus d'informations sur les paramètres du moteur ThreatSense, reportez-vous à la section Configuration des paramètres du moteur 10.

6.1.3.3 Quand faut-il modifier la configuration de la protection en temps réel ?

La protection en temps réel est le composant essentiel de la sécurisation du système à l'aide de ESET Cyber Security. Procédez avec prudence lorsque vous modifiez les paramètres de protection en temps réel. Il est recommandé de ne modifier ces paramètres que dans des cas très précis. Vous pouvez les modifier par exemple lorsqu'il y a conflit avec une autre application.

Après l'installation de ESET Cyber Security, tous les paramètres sont optimisés pour garantir le niveau maximum de système de sécurité aux utilisateurs. Pour restaurer les paramètres par défaut, cliquez sur **Par défaut** dans la partie inférieure gauche de la fenêtre **Protection en temps réel** (**Configuration** > **Saisie des préférences de l'application...** > **Protection en temps réel**).

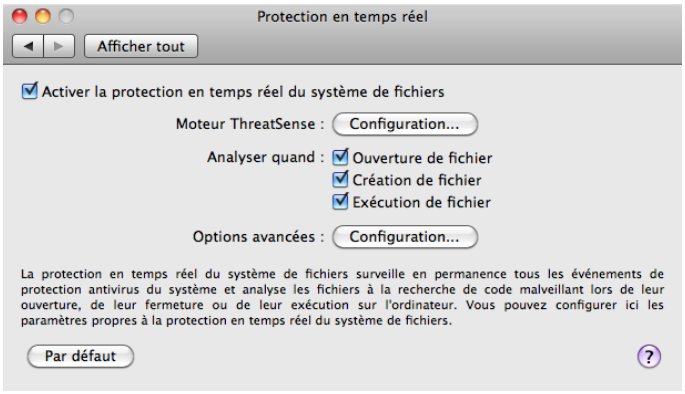
6.1.3.4 Vérification de la protection en temps réel

Pour vérifier que la protection en temps réel fonctionne et qu'elle détecte les virus éventuels, téléchargez le fichier de test eicar.com et vérifiez que ESET Cyber Security l'identifie en tant que menace. Ce fichier de test est un fichier inoffensif particulier qui est détectable par tous les programmes antivirus. Le fichier a été créé par l'institut EICAR (European Institute for Computer Antivirus Research) pour tester la fonctionnalité des programmes antivirus.

6.1.3.5 Que faire si la protection en temps réel ne fonctionne pas ?

Dans ce chapitre, nous décrivons des problèmes qui peuvent survenir lors de l'utilisation de la protection en temps réel et la façon de les résoudre.

La protection en temps réel est désactivée
Si la protection en temps réel est désactivée par inadvertance par un utilisateur, elle doit être réactivée. Pour réactiver la protection en temps réel, dans le menu principal, cliquez sur **Configuration** > **Ordinateur et réglez l'option Protection en temps réel du système de fichiers** sur **ACTIVÉ**. Vous pouvez également activer la protection en temps réel du système de fichiers dans la fenêtre des préférences de l'application : sous **Protection en temps réel**, sélectionnez **Activer la protection en temps réel du système de fichiers**.


Protection en temps réel
Afficher tout
Activer la protection en temps réel du système de fichiers
Moteur ThreatSense :
Configuration...
Analyser quand :
Ouverture de fichier
Création de fichier
Exécution de fichier
Options avancées :
Configuration...
La protection en temps réel du système de fichiers surveille en permanence tous les événements de protection antivirus du système et analyse les fichiers à la recherche de code malveillant lors de leur ouverture, de leur fermeture ou de leur exécution sur l'ordinateur. Vous pouvez configurer ici les paramètres propres à la protection en temps réel du système de fichiers.
Par défaut
?

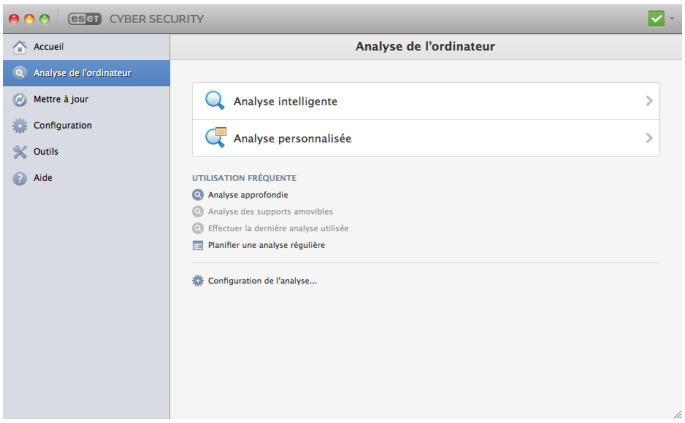
La protection en temps réel ne détecte et ne nettoie pas les infiltrations
Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si deux programmes de protection en temps réel sont activés en même temps, il peut y avoir un conflit entre les deux. Il est recommandé de désinstaller tout autre antivirus de votre système.

La protection en temps réel ne démarre pas
Si la protection en temps réel n'est pas initialisée au démarrage du système, cela peut provenir de conflits avec d'autres programmes. Dans ce cas, contactez le service client ESET.

6.1.4 Analyse de l'ordinateur à la demande

Si vous pensez que votre ordinateur peut être infecté (en raison d'un comportement anormal), exécutez une **analyse intelligente** pour rechercher d'éventuelles infiltrations. Pour une protection maximum, les analyses d'ordinateur doivent être exécutées régulièrement dans le cadre de mesures de sécurité de routine. Elles ne doivent pas être exécutées uniquement lorsqu'une infection est suspectée. Une analyse régulière peut détecter des infiltrations non détectées par l'analyseur en temps réel au moment de leur enregistrement sur le disque. Cela peut se produire si l'analyseur en temps réel est désactivé au moment de l'infection ou si la base de signatures de virus n'est plus à jour.

Nous recommandons d'exécuter une analyse de l'ordinateur à la demande au moins une fois par mois. L'analyse peut être configurée comme tâche planifiée dans **Outils** > **Planificateur**.



Vous pouvez également faire glisser les fichiers et dossiers sélectionnés sur votre Bureau ou dans la fenêtre du **Finder** et les faire glisser dans l'écran principal de ESET Cyber Security, sur l'icône du Dock, de la barre de menus (en haut de l'écran) ou de l'application (dans le dossier */Applications*).

6.1.4.1 Type d'analyse

Deux types d'analyses de l'ordinateur à la demande sont disponibles. L'**analyse intelligente** analyse le système sans exiger de configuration plus précise des paramètres d'analyse. L'**analyse personnalisée** permet de sélectionner l'un des profils d'analyse prédéfinis, ainsi que de choisir des cibles spécifiques à analyser.

6.1.4.1.1 Analyse intelligente

L'analyse intelligente permet de lancer rapidement une analyse de l'ordinateur et de nettoyer les fichiers infectés sans intervention de l'utilisateur. Elle présente l'avantage d'être facile à utiliser, sans aucune configuration d'analyse détaillée. L'analyse intelligente vérifie tous les fichiers de tous les dossiers, et nettoie ou supprime automatiquement les infiltrations détectées. Le niveau de nettoyage est automatiquement réglé sur sa valeur par défaut. Pour plus d'informations sur les types de nettoyage, reportez-vous à la section Nettoyage 11.

6.1.4.1.2 Analyse personnalisée

L'**analyse personnalisée** est la solution optimale si vous souhaitez spécifier des paramètres d'analyse tels que les cibles et les méthodes d'analyse. Elle permet en effet de configurer les paramètres avec grande précision. Les configurations peuvent être enregistrées sous forme de profils d'analyse définis par l'utilisateur, utiles pour effectuer régulièrement une analyse avec les mêmes paramètres.

Pour sélectionner des cibles à analyser, sélectionnez **Analyse de l'ordinateur** > **Analyse personnalisée**, puis des **cibles à analyser** spécifiques dans l'arborescence. Une cible à analyser peut également être spécifiée plus précisément : vous devez indiquer le chemin d'accès au dossier ou aux fichiers à inclure. Si vous souhaitez uniquement effectuer une analyse du système sans ajouter d'actions de nettoyage supplémentaires, sélectionnez **Analyse sans nettoyage**. Vous pouvez également choisir parmi trois niveaux de nettoyage en cliquant sur **Configuration...** > **Nettoyage**.

REMARQUE : L'exécution d'analyses personnalisées est recommandée pour les utilisateurs chevronnés qui maîtrisent l'utilisation de programmes antivirus.

6.1.4.2 Cibles à analyser

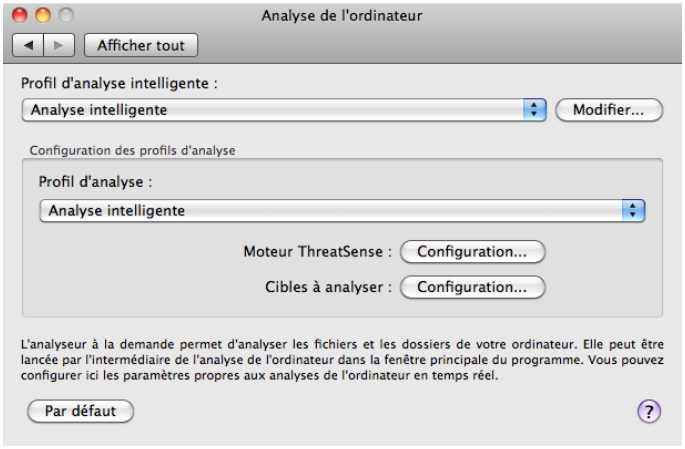
La structure arborescente des cibles à analyser permet de sélectionner les fichiers et dossiers à soumettre à l'analyse antivirus. Les dossiers peuvent également être sélectionnés en fonction des paramètres du profil.

Une cible à analyser peut aussi être définie plus précisément en entrant le chemin du dossier ou des fichiers à inclure dans l'analyse. Sélectionnez les cibles dans la structure arborescente qui répertorie tous les dossiers disponibles sur l'ordinateur en cochant la case qui correspond à un fichier ou un dossier donné.

6.1.4.3 Profils d'analyse

Vos paramètres d'analyse préférés peuvent être enregistrés pour les prochaines analyses. Il est recommandé de créer autant de profils (avec différentes cibles et méthodes, et d'autres paramètres d'analyse) que d'analyses utilisées régulièrement.

Pour créer un profil, sélectionnez dans le menu principal **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd+,*) > **Analyse de l'ordinateur** et cliquez sur l'option **Modifier...** en regarde de la liste des profils en cours.


Analyse de l'ordinateur
Afficher tout
Profil d'analyse intelligente :
Analyse intelligente
Modifier...
Configuration des profils d'analyse
Profil d'analyse :
Analyse intelligente
Moteur ThreatSense :
Configuration...
Cibles à analyser :
Configuration...
L'analyseur à la demande permet d'analyser les fichiers et les dossiers de votre ordinateur. Elle peut être lancée par l'intermédiaire de l'analyse de l'ordinateur dans la fenêtre principale du programme. Vous pouvez configurer ici les paramètres propres aux analyses de l'ordinateur en temps réel.
Par défaut

Pour plus d'informations sur la création d'un profil d'analyse, reportez-vous à la section Configuration des paramètres du moteur ThreatSense 10 ; vous y trouverez une description de chaque paramètre de configuration de l'analyse.

Exemple : Supposons la situation suivante : vous souhaitez créer votre propre profil d'analyse, la configuration d'analyse intelligente est partiellement adéquate, mais vous ne souhaitez analyser ni les fichiers exécutables compressés, ni les applications potentiellement dangereuses. Vous souhaitez effectuer un nettoyage strict. Dans la fenêtre **Liste des profils de l'analyseur à la demande**, saisissez le nom du profil, cliquez sur le bouton **Ajouter** et confirmez en cliquant sur **OK**. Réglez ensuite les paramètres pour qu'ils correspondent à vos besoins en configurant les options **Moteur ThreatSense** et **Cibles à analyser**.

Si vous souhaitez désactiver le système d'exploitation et mettre l'ordinateur hors tension une fois l'analyse à la demande terminée, utilisez l'option **Arrêter l'ordinateur après l'analyse**.

6.1.5 Configuration des paramètres du moteur ThreatSense

ThreatSense est une technologie ESET exclusive, constituée de plusieurs méthodes complexes de détection des menaces. Cette technologie est proactive : elle fournit une protection dès les premières heures de propagation d'une nouvelle menace. Elle utilise une combinaison de plusieurs méthodes (analyse de code, émulation de code, signatures génériques, signatures de virus) qui se conjuguent pour améliorer sensiblement la sécurité du système. Ce moteur d'analyse est capable de contrôler plusieurs flux de données simultanément, optimisant ainsi l'efficacité et le taux de détection. La technologie ThreatSense parvient également à bloquer les rootkits.

Les options de configuration de la technologie ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

- les types de fichiers et les extensions à analyser ;
- la combinaison de plusieurs méthodes de détection ;
- les niveaux de nettoyage, etc.

Pour afficher la fenêtre de configuration, sélectionnez **Configuration > Saisie des préférences de l'application...** (ou appuyez sur *cmd+,*), puis cliquez sur le bouton **Configuration du moteur ThreatSense...** situé dans les modules **Protection au démarrage**, **Protection en temps réel** et **Analyse de l'ordinateur**, qui utilisent tous la technologie ThreatSense (voir ci-dessous). Chaque scénario de sécurité peut exiger une configuration différente. ThreatSense est configurable individuellement pour les modules de protection suivants :

- **Protection au démarrage** : vérification automatique des fichiers de démarrage
- **Protection en temps réel** : protection en temps réel du système de fichiers
- **Analyse de l'ordinateur** : analyse de l'ordinateur à la demande
- **Protection de l'accès Web**
- **Protection de la messagerie**

Les paramètres ThreatSense sont optimisés pour chaque module et leur modification peut avoir une incidence significative sur le fonctionnement du système. Par exemple, en modifiant les paramètres pour toujours analyser les fichiers exécutables compressés ou pour activer l'analyse heuristique avancée dans le module de protection en temps réel du système de fichiers, vous pouvez dégrader les performances du système. Il est donc recommandé de ne pas modifier les paramètres ThreatSense par défaut pour tous les modules, à l'exception du module Analyse de l'ordinateur.

6.1.5.1 Objets

La section **Objets** permet de définir les fichiers qui vont faire l'objet d'une recherche d'infiltrations.

- **Liens symboliques** : (analyse de l'ordinateur uniquement) analyse les fichiers qui contiennent une chaîne de texte interprétée par le système d'exploitation comme un chemin d'accès à un autre fichier ou répertoire.
- **Fichiers de messagerie** : (non disponible dans la protection en temps réel) analyse les fichiers de messagerie.
- **Boîtes aux lettres** : (non disponible dans la protection en temps réel) analyse les boîtes aux lettres de l'utilisateur stockées dans le système. L'utilisation inadéquate de cette option peut provoquer des conflits avec votre client de messagerie. Pour en savoir plus sur les avantages et les inconvénients de cette option, reportez-vous à cet article de base de connaissances.
- **Archives** : (non disponible dans la protection en temps réel) analyse les fichiers compressés dans les archives (.rar, .zip, .arj, .tar, etc.).
- **Archives auto-extractibles** : (non disponible dans la protection en temps réel) analyse les fichiers contenus dans des fichiers d'archives auto-extractibles.
- **Fichiers exécutables compressés** : contrairement aux types d'archives standard, les fichiers exécutables compressés sont décompressés en mémoire. Lorsque cette option est sélectionnée, les fichiers exécutables compressés statiques standard (ex. : UPX, yoda, ASPack, FGS) sont également analysés.

6.1.5.2 Options

Dans la section **Options**, vous pouvez sélectionner les méthodes utilisées lors d'une analyse du système. Les options disponibles sont les suivantes :

- **Heuristique** : l'heuristique est un algorithme qui analyse l'activité (malveillante) des programmes. La détection heuristique présente l'avantage de détecter les nouveaux logiciels malveillants qui n'existaient pas auparavant ou qui ne figurent pas dans la liste des virus connus (base de signatures de virus).
- **Heuristique avancée** : cette option utilise un algorithme heuristique unique développé par ESET et optimisé pour la détection de vers informatiques et de chevaux de Troie écrits dans des langages de programmation de haut niveau. L'heuristique avancée améliore de manière significative la capacité de détection du programme.

6.1.5.3 Nettoyage

Les paramètres de nettoyage déterminent la façon dont l'analyseur nettoie les fichiers infectés. Trois niveaux de nettoyage sont possibles :

- **Pas de nettoyage** : les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche une fenêtre d'alerte et permet à l'utilisateur de choisir une action.
- **Nettoyage standard** : le programme essaie de nettoyer ou de supprimer automatiquement tout fichier infecté. S'il n'est pas possible de sélectionner automatiquement l'action requise, le programme propose une sélection d'actions de suivi. Cette sélection s'affiche également si une action prédéfinie ne peut pas être menée à bien.
- **Nettoyage strict** : le programme nettoie ou supprime tous les fichiers infectés (y compris les archives). Les seules exceptions sont les fichiers système. S'il n'est pas possible de nettoyer un fichier, vous recevez une notification et êtes invité à sélectionner le type d'action à exécuter.

Avertissement : dans le mode de nettoyage standard par défaut, les fichiers d'archive ne sont entièrement supprimés que si tous les fichiers qu'ils contiennent sont infectés. Si une archive contient des fichiers valides et des fichiers infectés, elle n'est pas supprimée. Si un fichier d'archive infecté est détecté dans le mode Nettoyage strict, le fichier entier est supprimé, même s'il contient également des fichiers intacts.

6.1.5.4 Exclusions

L'extension est la partie du nom d'un fichier située après le point. Elle définit le type et le contenu d'un fichier. Cette section de la configuration des paramètres ThreatSense vous permet de définir les types de fichiers à exclure de l'analyse.

Par défaut, tous les fichiers sont analysés, quelle que soit leur extension. Toutes les extensions peuvent être ajoutées à la liste des fichiers exclus de l'analyse. Les boutons + et − permettent d'activer ou d'empêcher l'analyse d'extensions spécifiques.

L'exclusion de certains fichiers de l'analyse peut être utile si l'analyse de ces fichiers provoque un dysfonctionnement du programme. Par exemple, il peut être judicieux d'exclure les extensions *log*, *cfg* et *tmp*. Le format correct de saisie des extensions de fichiers est le suivant :
log
cfg
tmp

6.1.5.5 Limites

La section **Limites** permet de spécifier la taille maximale des objets et les niveaux d'imbrication des archives à analyser :

- **Taille maximale :** définit la taille maximum des objets à analyser. Une fois la taille maximale définie, le module antivirus analysera uniquement les objets dont la taille est inférieure à la taille spécifiée. Cette option ne doit être modifiée que par des utilisateurs chevronnés ayant des raisons très précises d'exclure de l'analyse les objets plus volumineux.
- **Durée maximale d'analyse :** définit la durée maximum attribuée à l'analyse d'un objet. Si la valeur de ce champ a été définie par l'utilisateur, le module antivirus cesse d'analyser un objet une fois ce temps écoulé, que l'analyse soit terminée ou non.
- **Niveau d'imbrication maximal :** indique la profondeur maximale d'analyse des archives. Il n'est pas recommandé de modifier la valeur par défaut (10). Dans des circonstances normales, il n'y a aucune raison de le faire. Si l'analyse prend fin prématurément en raison du nombre d'archives imbriquées, l'archive reste non vérifiée.
- **Taille de fichiers maximale :** cette option permet de spécifier la taille maximale (après extraction) des fichiers à analyser qui sont contenus dans les archives. Si l'analyse prend fin prématurément en raison de cette limite, l'archive reste non vérifiée.

6.1.5.6 Autres

Activer l'optimisation intelligente
Lorsque l'option Optimisation intelligente est activée, les paramètres sont optimisés de manière à garantir le niveau d'analyse le plus efficace sans compromettre la vitesse d'analyse. Les différents modules de protection proposent une analyse intelligente en utilisant différentes méthodes. L'option Optimisation intelligente n'est pas définie de manière fixe dans le produit. L'équipe de développement d'ESET Development Team met en œuvre en permanence de nouvelles modifications qui sont ensuite intégrées dans ESET Cyber Security par l'intermédiaire de mises à jour régulières. Si l'option Optimisation intelligente est désactivée, seuls les paramètres définis par l'utilisateur dans le noyau ThreatSense de ce module particulier sont appliqués lors de la réalisation d'une analyse.

Analyser l'autre flux de données (analyseur à la demande uniquement)
Les autres flux de données (branchements de ressources/ données) utilisés par le système de fichiers sont des associations de fichiers et de dossiers invisibles pour les techniques ordinaires de détection de virus. De nombreuses infiltrations tentent d'éviter la détection en se faisant passer pour d'autres flux de données.

6.1.6 Une infiltration est détectée

Des infiltrations peuvent atteindre le système à partir de différents points d'entrée : pages Web, dossiers partagés, courrier électronique ou périphériques amovibles (USB, disques externes, CD, DVD, etc.).

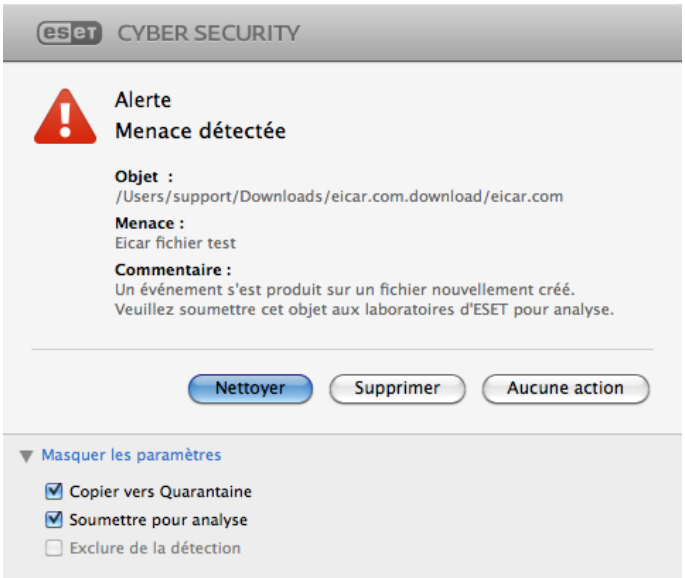
Si votre ordinateur montre des signes d'infection par un logiciel malveillant (par exemple des ralentissement, des blocages fréquents, etc.), nous vous recommandons d'effectuer les opérations suivantes :

1. Cliquez sur **Analyse de l'ordinateur**.
2. Cliquez sur **Analyse intelligente** (pour plus d'informations, reportez-vous à la section Analyse intelligente 9).
3. Lorsque l'analyse est terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés.

Si vous ne souhaitez analyser qu'une certaine partie de votre disque, cliquez sur **Analyse personnalisée** et sélectionnez les cibles à analyser.

Pour donner un exemple général du traitement des infiltrations par ESET Cyber Security, supposons qu'une infiltration soit détectée par la protection en temps réel du système de fichiers, qui utilise le niveau de nettoyage par défaut. La protection en temps réel va tenter de nettoyer ou de supprimer le fichier. Si aucune action n'est prédéfinie pour le module de protection en temps réel, vous êtes invité à sélectionner une option dans une fenêtre d'alerte. Généralement, les options **Nettoyer**, **Supprimer** et **Aucune action** sont disponibles. Il n'est pas recommandé de sélectionner **Aucune action**, car les fichiers infectés seraient conservés dans leur état infecté. Cette option concerne les situations où vous êtes sûr que le fichier est inoffensif et a été détecté par erreur.

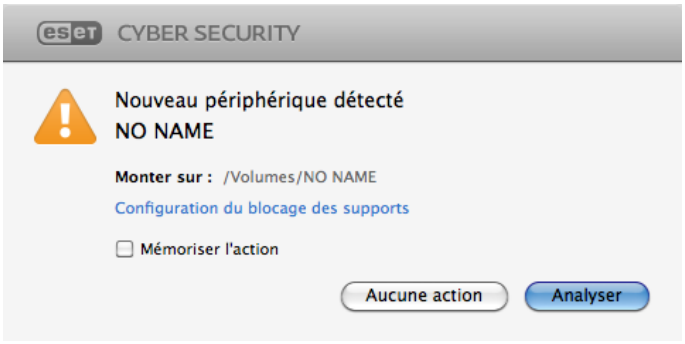
Nettoyage et suppression : utilisez le nettoyage si un fichier a été attaqué par un virus qui y a joint du code malveillant. Dans ce cas, essayez d'abord de nettoyer le fichier infecté pour le restaurer dans son état d'origine. Si le fichier se compose uniquement de code malveillant, il sera supprimé.



Suppression de fichiers dans des archives : en mode de nettoyage par défaut, l'archive complète n'est supprimée que si elle ne contient que des fichiers infectés et aucun fichier sain. Autrement dit, les archives ne sont pas supprimées si elles contiennent également des fichiers sains. Cependant, soyez prudent si vous choisissez un **nettoyage strict** : dans ce mode, l'archive est supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

6.2 Analyse et blocage de supports amovibles

ESET Cyber Security peut exécuter une analyse à la demande du support amovible introduit (CD, DVD, USB, périphérique iOS, etc.).



Les supports amovibles peuvent contenir du code malveillant et constituer un risque pour votre ordinateur. Pour bloquer des supports amovibles, cliquez sur **Configuration du blocage des supports** (voir l'illustration ci-dessus) ou sur **Configuration** > **Saisie des préférences de l'application...** > **Supports** dans la fenêtre principale du programme et sélectionnez **Activer le blocage des supports amovibles**. Pour autoriser l'accès à certains types de supports, désélectionnez les volumes souhaités.

REMARQUE : Pour autoriser l'accès à un lecteur de CD-ROM externe connecté à votre ordinateur par le biais d'un câble USB, désélectionnez l'option **CD-ROM**.

7. Antihameçonnage

Le terme *hameçonnage* (en anglais : phishing) définit une activité criminelle basée sur l'ingénierie sociale (c'est-à-dire la manipulation des personnes pour leur soutirer des informations confidentielles). Le hameçonnage est souvent utilisé pour obtenir l'accès à des données sensibles telles que des numéros de comptes bancaires, des numéros de cartes de paiement, des codes PIN ou des noms d'utilisateur ainsi que leur mot de passe.

Nous vous recommandons de maintenir activé l'antihameçonnage (**Configuration** > **Saisie des préférences de l'application...** > **Protection Anti-Phishing**). Toutes les attaques par hameçonnage potentielles en provenance de sites Web ou de domaines référencés dans la base de logiciels malveillants d'ESET seront bloquées. Une notification d'avertissement sera également affichée pour vous informer de l'attaque.

8. Protection Internet et de la messagerie

Pour accéder à la protection Internet et de la messagerie, cliquez dans le menu principal sur **Configuration** > **Internet et messagerie**. Vous pouvez également accéder aux paramètres détaillés de chaque module en cliquant sur **Configuration...**

Protection de l'accès Web : surveille la communication entre les navigateurs et les serveurs distants.

Protection du client de messagerie : permet de contrôler la communication par courrier électronique effectuée via les protocoles POP3 et IMAP.

Protection Anti-Phishing : bloque les éventuelles attaques de hameçonnage en provenance de sites Web ou domaines répertoriés dans la base de données ESET des logiciels malveillants.

8.1 Protection Web

La protection de l'accès Web surveille les communications entre les navigateurs Web et les serveurs distants et respecte les règles du protocole HTTP (Hypertext Transfer Protocol).

8.1.1 Ports

L'onglet **Ports** permet de définir les numéros de port utilisés pour les communications HTTP. Par défaut, les numéros de port 80, 8080 et 3128 sont prédéfinis.

8.1.2 Mode actif

ESET Cyber Security contient également le sous-menu **Mode actif**, qui définit le mode de contrôle des navigateurs Web. Le mode actif examine les données transférées à partir d'applications accédant à Internet en général, qu'elles soient ou nom qualifiées de navigateurs Web. S'il n'est pas activé, les communications des applications sont surveillées progressivement par lots. Cela réduit l'efficacité de la vérification des données, mais assure aussi une plus grande compatibilité des applications. Si aucun problème ne se produit lors de son utilisation, nous recommandons d'activer le mode actif en cochant la case en regard de l'application concernée.

Lorsqu'une application contrôlée télécharge des données, celles-ci sont d'abord enregistrées dans un fichier temporaire créé par ESET Cyber Security. À ce stade, les données ne sont pas disponibles pour l'application en question. Une fois que le téléchargement est terminé, les données sont soumises à une recherche de code malveillant. Si aucune infiltration n'est détectée, les données sont envoyées à l'application d'origine. Ce processus assure un contrôle complet des communications d'une application contrôlée. Si le mode passif est activé, les données sont fournies peu à peu à l'application d'origine pour éviter les expirations de délais.

8.1.3 Listes d'URL

La section **Listes d'URL** permet de spécifier des adresses HTTP à bloquer, à autoriser ou à exclure du contrôle. Les sites Web figurant dans la liste des adresses bloquées ne seront pas accessibles. Les sites Web répertoriés dans la liste des adresses exclues sont accessibles sans recherche de code malveillant.

Pour réserver l'accès aux adresses URL figurant dans la liste des **URL autorisées**, sélectionnez l'option **Limiter les adresses URL**.

Pour activer une liste, sélectionnez l'option **Activé** située en regard du nom de la liste. Si vous souhaitez être averti lors de la saisie d'une adresse figurant dans la liste courante, sélectionnez **Notifiée**.

Dans n'importe quelle liste, vous pouvez utiliser les symboles spéciaux *(astérisque) et ?(point d'interrogation). L'astérisque remplace toute chaîne de caractères, tandis que le point d'interrogation remplace n'importe quel caractère. Soyez particulièrement prudent dans la définition des adresses exclues, car la liste ne doit contenir que des adresses fiables et sûres. De même, il faut veiller à utiliser correctement les symboles * et ? dans cette liste.

8.2 Protection de la messagerie

La protection de la messagerie permet de contrôler la communication par courrier électronique effectuée via les protocoles POP3 et IMAP. Lorsqu'il examine les messages entrants, le programme utilise toutes les méthodes d'analyse avancées comprises dans le moteur d'analyse ThreatSense. La détection des programmes malveillants s'effectue donc avant même leur comparaison avec la base des signatures de virus. L'analyse des communications suivant les protocoles POP3 et IMAP est indépendante du client de messagerie utilisé.

Moteur ThreatSense : la configuration avancée de l'analyseur de virus permet de configurer les cibles à analyser, les méthodes de détection, etc. Cliquez sur **Configuration...** pour afficher la fenêtre de configuration détaillée de l'analyseur.

Ajouter la notification à la note de bas de page du message : utilisez cette option pour insérer une alerte de virus dans le message infecté. Cette fonctionnalité permet un filtrage simple des messages infectés. Elle augmente aussi le niveau de crédibilité vis-à-vis du destinataire et, en cas de détection d'une infiltration, elle fournit des informations précieuses sur le niveau de menace d'un message ou d'un expéditeur donné. Les options suivantes sont disponibles :

Jamais : aucune notification ne sera ajoutée ;
Courriers infectés uniquement : seuls les messages contenant des logiciels malveillants seront marqués comme vérifiés ;
Tous les courriers analysés : le programme ajoute une notification à chaque message analysé.

Après la vérification d'un message, une notification peut y être ajoutée avec les résultats de l'analyse. Vous pouvez sélectionner **Ajouter une note à l'objet du courrier infecté reçu et lu**. Ne vous fiez pas aveuglément à ces notifications, car elles peuvent ne pas figurer dans des messages HTML problématiques ou être contrefaites par certains virus.

Modèle ajouté à l'objet du courrier infecté : modifiez ce modèle pour changer le format du préfixe ajouté à l'objet d'un message infecté.

8.2.1 Vérification par protocole POP3

Le protocole POP3 est le protocole le plus répandu pour la réception de courrier électronique dans un client de messagerie. ESET Cyber Security assure la protection de ce protocole quel que soit le client de messagerie utilisé.

Le module de protection assurant cette vérification est automatiquement lancé au démarrage du système et reste ensuite actif en mémoire. Vérifiez que le module est activé pour que le filtrage des protocoles fonctionne correctement ; la vérification par protocole POP3 est effectuée automatiquement sans qu'il soit nécessaire de reconfigurer le client de messagerie. Par défaut, toutes les communications sur le port 110 sont analysées, mais vous pouvez y ajouter d'autres ports de communication au besoin. Les numéros de ports doivent être séparés par des virgules.

Si l'option **Activer la vérification par protocole POP3** est activée, tout le trafic POP3 fait l'objet d'un contrôle des logiciels malveillants.

8.2.2 Vérification par protocole IMAP

Le protocole IMAP (Internet Message Access Protocol) est un autre protocole Internet destiné à la récupération de courrier électronique. IMAP présente certains avantages par rapport à POP3. Il permet notamment la connexion simultanée de plusieurs clients à la même boîte aux lettres et permet de conserver les informations d'état des messages telles que le fait de savoir si le message a été lu, si une réponse a été envoyée ou s'il a été supprimé. ESET Cyber Security offre une protection pour ce protocole quel que soit le client de messagerie utilisé.

Le module de protection assurant cette vérification est automatiquement lancé au démarrage du système et reste ensuite actif en mémoire. Assurez-vous que la vérification par protocole IMAP est activée pour que le module fonctionne correctement ; le contrôle du protocole IMAP est effectué automatiquement sans qu'il soit nécessaire de reconfigurer le client de messagerie. Par défaut, toutes les communications sur le port 143 sont analysées, mais vous pouvez y ajouter d'autres ports de communication au besoin. Les numéros de ports doivent être séparés par des virgules.

Si l'option **Activer la vérification par protocole IMAP** est activée, tout le trafic IMAP fait l'objet d'un contrôle des logiciels malveillants.

9. Mettre à jour

Des mises à jour régulières de ESET Cyber Security sont nécessaires pour conserver le niveau maximum de sécurité. Le module de mise à jour garantit que le programme est toujours à jour en téléchargeant la dernière version de la base de signatures de virus.

Cliquez sur **Mettre à jour** dans le menu principal pour afficher l'état actuel de la mise à jour de ESET Cyber Security, notamment la date et l'heure de la dernière mise à jour. Vous pouvez également savoir si une mise à jour est nécessaire. Pour démarrer manuellement la mise à jour, cliquez sur **Mettre à jour la base de signatures de virus**.

Dans des circonstances normales, lorsque des mises à jour sont correctement téléchargées, le message **La mise à jour n'est pas nécessaire : la base de signatures de virus installée est à jour** apparaîtra dans la fenêtre Mettre à jour. Si la base de signatures de virus ne peut pas être mise à jour, il est recommandé de vérifier les paramètres de mise à jour 14. Cette erreur est généralement liée à la saisie incorrecte de données d'authentification (nom d'utilisateur et mot de passe) ou à la configuration incorrecte des paramètres de connexion 20.

La fenêtre Mettre à jour contient également la version de la base de signatures de virus. Cette indication numérique est un lien actif vers le site Web d'ESET qui répertorie toutes les signatures ajoutées dans cette mise à jour.

REMARQUE : Votre nom d'utilisateur et votre mot de passe vous sont fournis par ESET après l'achat de ESET Cyber Security.

9.1 Configuration des mises à jour

L'authentification auprès du serveur de mises à jour ESET est basée sur le nom d'utilisateur et le mot de passe qui ont été générés et vous ont été transmis après votre achat.

Pour activer l'utilisation du mode test (téléchargement des mises à jour des versions précommerciales), cliquez sur le bouton **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd+,*) > **Mettre à jour**, cliquez sur **Configuration...** en regard de l'option **Options avancées** et cochez ensuite la case **Activer le mode test**. Nous vous recommandons d'utiliser le mode test uniquement lorsqu'une mise à jour anticipée est disponible pour résoudre un problème que vous rencontrez avec ESET Cyber Security.

Mettre à jour
Afficher tout
Nom d'utilisateur :
EAV-12345678
Mot de passe :
Afficher le mot de passe
Options avancées :
Configuration...
Effacer le cache de mise à jour :
Effacer
Pour que le programme puisse fournir une protection complète contre les menaces, il est essentiel que la base de signatures de virus soit toujours à jour. Vous pouvez configurer ici les paramètres de mise à jour.
Par défaut

Pour supprimer toutes les données de mise à jour stockées temporairement, cliquez sur le bouton **Effacer** situé en regard de l'option **Effacer le cache de mise à jour**. Utilisez cette option si vous rencontrez des problèmes de mise à jour.

9.1.1 Configuration avancée

Pour désactiver les notifications affichées après chaque mise à jour, sélectionnez **Ne pas afficher de notification de réussite des mises à jour**.

Activez **le mode test** pour télécharger des modules en cours de développement qui ont fait l'objet de tests finaux. Les mises à jour des versions précommerciales contiennent souvent des correctifs qui résolvent les problèmes du produit. L'option **Mise à jour reportée** permet de télécharger les mises à jour quelques heures après leur publication pour s'assurer que les clients ne recevront pas de mises à jour comportant des problèmes.

ESET Cyber Security enregistre des instantanés de la base des signatures de virus et des modules du programme afin de les

utiliser avec la fonctionnalité **Restauration des mises à jour**. Conservez l'option **Créer des instantanés des fichiers de mise à jour** activée pour qu'ESET Cyber Security enregistre automatiquement ces instantanés. Si vous pensez qu'une nouvelle mise à jour de la base des virus et/ou des modules du programme peut être instable ou endommagée, vous pouvez restaurer la version précédente et désactiver les mises à jour pendant une période définie. Vous pouvez également activer les mises à jour précédemment désactivées si vous les avez reportées indéfiniment. Lors de la restauration d'une mise à jour précédente, utilisez le menu déroulant **Définir la période d'interruption sur** pour spécifier la période d'interruption des mises à jour. Si vous sélectionnez **jusqu'à révocation**, les mises à jour normales ne reprendront pas une fois que vous les aurez manuellement restaurées. Procédez avec prudence lorsque vous sélectionnez ce paramètre.

Définir automatiquement l'âge maximal de la base de données : permet de définir le délai maximal (en jour) au terme duquel la base des signatures de virus est signalée comme étant obsolète. La valeur par défaut est 7 jours.

9.2 Comment créer des tâches de mise à jour

Vous pouvez déclencher manuellement les mises à jour en cliquant sur **Mettre à jour** dans le menu principal, puis sur **Mettre à jour la base des signatures de virus**.

Les mises à jour peuvent également être exécutées sous forme de tâches planifiées. Pour configurer une tâche planifiée, cliquez sur **Outils** > **Planificateur**. Par défaut, les tâches suivantes sont activées dans ESET Cyber Security :

- **Mise à jour automatique régulière**
- **Mise à jour automatique après ouverture de session utilisateur**

Chacune des tâches de mise à jour peut être modifiée selon les besoins de l'utilisateur. Outre les tâches de mise à jour par défaut, vous pouvez créer de nouvelles tâches avec votre propre configuration. Pour plus d'informations sur la création et la configuration des tâches de mise à jour, reportez-vous à la section Planificateur 16.

9.3 Mise à jour de ESET Cyber Security vers une nouvelle version

Pour bénéficier d'une protection maximale, il est important d'utiliser la dernière version de ESET Cyber Security. Pour rechercher une nouvelle version, cliquez sur **Accueil** dans le menu principal. Si une nouvelle version est disponible, un message s'affiche. Cliquez sur **En savoir plus...** pour afficher une nouvelle fenêtre contenant le numéro de la nouvelle version et la liste des modifications.

Cliquez sur **Oui** pour télécharger la dernière version ou cliquez sur **Pas maintenant** pour fermer la fenêtre et télécharger la mise à niveau ultérieurement.

Si vous cliquez sur **Oui**, le fichier est téléchargé dans le dossier des téléchargements (ou dans le dossier par défaut défini par votre navigateur). Lorsque le téléchargement du fichier est terminé, lancez le fichier et suivez les instructions d'installation. Votre nom d'utilisateur et votre mot de passe sont transférés automatiquement vers la nouvelle installation. Il est recommandé de vérifier régulièrement si des mises à niveau sont disponibles, en particulier si vous installez ESET Cyber Security à partir d'un CD ou d'un DVD.

9.4 Mises à jour du système

La fonctionnalité de mise à jour du système Mac OS X est un composant important conçu pour protéger les utilisateurs des logiciels malveillants. Pour une sécurité maximale, nous vous recommandons d'installer ces mises à jour dès qu'elles sont disponibles. En fonction du niveau de sécurité que vous indiquez, ESET Cyber Security vous indiquera les mises à jour manquantes. Vous pouvez ajuster les notifications de disponibilité des mises à jour dans **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd+,*) > **Alertes et notifications** > **Configuration...** en modifiant les options **Conditions d'affichage** situées en regard de l'option **Mises à jour du système d'exploitation**.

- **Afficher toutes les mises à jour** : une notification s'affiche dès qu'une mise à jour système est manquante
- **Afficher uniquement les mises à jour recommandées** : vous êtes informé des mises à jour recommandées uniquement

Si vous ne souhaitez pas être informé de l'absence de mises à jour, désélectionnez la case située à côté de **Mises à jour du système d'exploitation**.

La fenêtre de notification présente les mises à jour disponibles pour le système d'exploitation Mac OS X, ainsi que les applications mises à jour par l'outil Software updates natif de Mac OS X. Vous pouvez exécuter la mise à jour directement depuis la fenêtre de notification ou à partir de la section **Accueil** de ESET Cyber Security en cliquant sur l'option d'**installation des mises à jour manquantes**.

La fenêtre de notification contient le nom, la version, la taille et les propriétés (marqueurs) de l'application, ainsi que d'autres informations sur les mises à jour disponibles. La colonne **Marqueurs** contient les informations suivantes :

- **[recommended]** : le fabricant du système d'exploitation recommande d'installer cette mise à jour pour améliorer la sécurité et la stabilité du système.
- **[restart]** : l'ordinateur doit être redémarré après l'installation.
- **[shutdown]** : l'ordinateur doit être arrêté, puis redémarré après l'installation.

La fenêtre de notification indique les mises à jour récupérées par l'outil de ligne de commande 'softwareupdate'. Les mises à jour récupérées par cet outil peuvent être différentes de celles affichées par l'application Software updates. Si vous souhaitez installer toutes les mises à jour disponibles qui sont répertoriées dans la fenêtre des mises à jour système manquantes, vous devez utiliser l'outil de ligne de commande 'softwareupdate'. Pour en savoir plus sur cet outil, consultez le manuel « softwareupdate » en saisissant `man softwareupdate` dans une **fenêtre de terminal**. Cette option est recommandée uniquement pour les utilisateurs chevronnés.

10. Outils

Le menu **Outils** contient des modules qui simplifient l'administration du programme et offrent des options supplémentaires pour les utilisateurs chevronnés.

10.1 Fichiers journaux

Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées. La consignation (enregistrement dans les fichiers journaux) représente un puissant outil pour l'analyse système, la détection de menaces et le dépannage. La consignation est toujours active en arrière-plan, sans interaction de l'utilisateur. Les informations sont enregistrées en fonction des paramètres de verbosité. Il est possible de consulter les messages texte et les journaux, ainsi que d'archiver les journaux, directement à partir de l'environnement ESET Cyber Security.

Vous pouvez accéder aux fichiers journaux depuis le menu principal ESET Cyber Security en cliquant sur **Outils** > **Journaux**. Sélectionnez le type de journal souhaité dans le menu déroulant **Journal**, en haut de la fenêtre. Les journaux suivants sont disponibles :

1. **Menaces détectées** : cette option permet de consulter toutes les informations concernant les événements liés à la détection d'infiltrations.
2. **Événements** : cette option permet aux administrateurs système et aux utilisateurs de résoudre des problèmes. Toutes les actions importantes exécutées par ESET Cyber Security sont enregistrées dans les journaux des événements.
3. **Analyse de l'ordinateur** : ce journal affiche les résultats de toutes les analyses effectuées. Pour afficher les détails d'une analyse de l'ordinateur à la demande, double-cliquez sur l'entrée correspondante.

Vous pouvez copier les informations affichées dans chaque section directement dans le Presse-papiers en sélectionnant l'entrée souhaitée, puis en cliquant sur le bouton **Copier**.

10.1.1 Maintenance des journaux

La configuration de la consignation de ESET Cyber Security est accessible à partir de la fenêtre principale du programme. Cliquez sur **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd+,*) > **Fichiers journaux**. Les options suivantes peuvent être spécifiées pour les fichiers journaux :

- **Supprimer les anciennes entrées du journal automatiquement** : les entrées de journal plus anciennes que le nombre de jours spécifié sont automatiquement supprimées.
- **Optimiser automatiquement les fichiers journaux** : permet la défragmentation automatique des fichiers journaux si le pourcentage spécifié d'enregistrements inutilisés est dépassé.

Pour configurer l'option **Filtre par défaut des entrées du journal**, cliquez sur **Modifier...** et sélectionnez/désélectionnez les types de journaux en fonction de vos besoins.

10.1.2 Filtrage des journaux

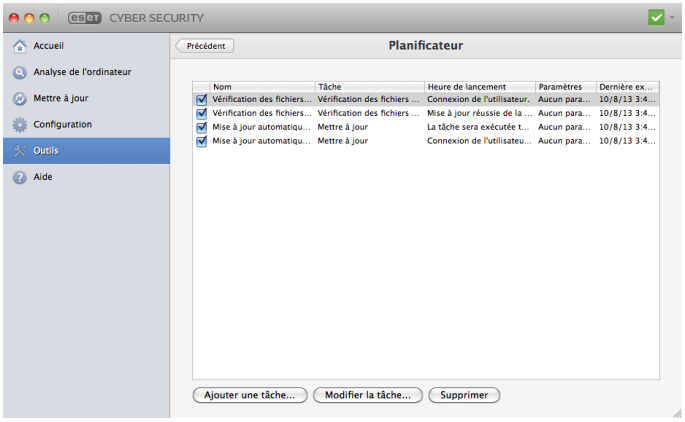
Les journaux stockent des informations sur les événements système importants : La fonctionnalité de filtrage des journaux permet d'afficher des entrées concernant un type d'événement spécifique.

Les types de journaux les plus fréquemment utilisés sont répertoriés ci-dessous :

- **Avertissements critiques** : erreurs système critiques (par exemple, le démarrage de la protection antivirus a échoué).
- **Erreurs** : messages d'erreur du type *Erreur de téléchargement de fichier* et erreurs critiques.
- **Avertissements** : messages d'avertissement.
- **Entrées informatives** : messages d'informations concernant des mises à jour, des alertes, etc.
- **Entrées de diagnostic** : informations nécessaires au réglage du programme et de toutes les entrées décrites ci-dessus.

10.2 Planificateur

Le **planificateur** est accessible depuis le menu principal de ESET Cyber Security, dans **Outils**. Le **planificateur** contient la liste de toutes les tâches planifiées et des propriétés de configuration telles que la date et l'heure prédéfinies, ainsi que le profil d'analyse utilisé.



Le planificateur gère et lance les tâches planifiées qui ont été préalablement définies et configurées. La configuration et les propriétés comprennent des informations telles que la date et l'heure, ainsi que des profils spécifiques à utiliser pendant l'exécution de ces tâches.

Par défaut, les tâches planifiées suivantes sont affichées dans le planificateur :

- Maintenance des journaux (une fois que l'option **Afficher les tâches système** est activée dans la configuration du planificateur)
- Vérification des fichiers de démarrage après ouverture de session utilisateur
- Vérification des fichiers de démarrage après mise à jour réussie de la base de signatures de virus

- Mise à jour automatique régulière
- Mise à jour automatique après ouverture de session utilisateur

Pour modifier la configuration d'une tâche planifiée existante (par défaut ou définie par l'utilisateur), appuyez sur Ctrl et cliquez sur la tâche à modifier, puis sélectionnez **Modifier…**. Vous pouvez également sélectionner la tâche et cliquer sur le bouton **Modifier la tâche…** .

10.2.1 Création de nouvelles tâches

Pour créer une nouvelle tâche dans le planificateur, cliquez sur **Ajouter une tâche…** ou appuyez sur la touche CTRL et cliquez dans le champ vierge, puis sélectionnez **Ajouter…** dans le menu contextuel. Cinq types de tâches planifiées sont disponibles :

- **Exécuter l'application**
- **Mettre à jour**
- **Maintenance des journaux**
- **Analyse de l'ordinateur à la demande**
- **Vérification des fichiers de démarrage du système**

REMARQUE : en choisissant **Exécuter l'application**, vous pouvez exécuter des programmes en tant qu'utilisateur système appelé « nobody ». Les autorisations d'exécution des applications par l'intermédiaire du Planificateur sont définies par Mac OS X.

Dans l'exemple ci-dessous, nous allons utiliser le Planificateur pour ajouter une nouvelle tâche de mise à jour, car c'est l'une des tâches planifiées les plus utilisées :

1. Dans le menu déroulant **Tâche planifiée**, sélectionnez **Mettre à jour**.
2. Saisissez le nom de la tâche dans le champ **Nom de la tâche**.
3. Sélectionnez la fréquence de la tâche dans le menu déroulant **Exécuter la tâche**. Selon la fréquence sélectionnée, vous êtes invité à indiquer différents paramètres de mise à jour. Si vous sélectionnez **Définie par l'utilisateur**, le système vous invite à indiquer la date et l'heure au format cron (pour plus d'informations, reportez-vous à la section Création d'une tâche définie par l'utilisateur 17).
4. À l'étape suivante, définissez l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée.
5. Dans la dernière étape, une fenêtre récapitulative apparaît ; elle affiche des informations sur la tâche planifiée en cours. Cliquez sur **Terminer**. La nouvelle tâche planifiée est ajoutée à la liste des tâches planifiées.

Par défaut, ESET Cyber Security contient les tâches planifiées prédéfinies qui garantissent le fonctionnement correct du produit. Ces tâches ne doivent pas être modifiées et sont masquées par défaut. Pour que ces tâches soient visibles, sélectionnez dans le menu principal **Configuration** > **Saisie des préférences de l'application…** (ou appuyez sur *cmd+,*) > **Planificateur** et sélectionnez l'option **Afficher les tâches système**.

10.2.2 Création de tâches définies par l'utilisateur

La date et l'heure de la tâche **Définie par l'utilisateur** doivent être indiquées au format cron sur l'année (chaîne composée de 6 champs séparés par un espace) :
`minute(0-59) heure(0-23) jour du mois(1-31) mois (1-12) année(1970-2099) jour de la semaine(0-7) (dimanche = 0 ou 7)`

Exemple :
`30 6 22 3 2012 4`

Caractères spéciaux pris en charge dans les expressions cron :
- astérisque (`*`) - l'expression correspond à toutes les valeurs du champ ; par exemple, un astérisque dans le 3e champ (jour du mois) signifie « tous les jours »
- tiret (`-`) - définit des plages ; par exemple, `3-9`
- virgule (`,`) - sépare les éléments d'une liste ; par exemple, `1,3,7,8`
- barre oblique (`/`) - définit des incréments de plages ; par exemple, `3-28/5` dans le 3e champ (jour du mois) indique le 3e jour du mois, puis une fréquence tous les 5 jours.

Les noms de jour (Monday-Sunday) et de mois (January-December) ne sont pas pris en charge.

REMARQUE : si vous définissez un jour du mois et un jour de la semaine, la commande n'est exécutée que si les deux champs correspondent.

10.3 Quarantaine

La principale fonction de la quarantaine consiste à stocker les fichiers infectés en toute sécurité. Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer ou s'ils sont détectés erronément par ESET Cyber Security.

Vous pouvez choisir de mettre n'importe quel fichier en quarantaine. Cette action est conseillée si un fichier se comporte de façon suspecte mais n'a pas été détecté par l'analyseur antivirus. Les fichiers de la quarantaine peuvent être soumis pour analyse au laboratoire de recherche sur les menaces d'ESET.

Les fichiers du dossier de quarantaine sont répertoriés dans un tableau qui affiche la date et l'heure de mise en quarantaine, le chemin de l'emplacement d'origine du fichier infecté, sa taille en octets, la raison (par exemple « ajouté par l'utilisateur ») et le nombre de menaces (par exemple, s'il s'agit d'une archive contenant plusieurs infiltrations). Le dossier de quarantaine dans lequel sont stockés les fichiers en quarantaine (*/Library/Application Support/Eset/esets/cache/quarantine*) reste dans le système même après la désinstallation de ESET Cyber Security. Les fichiers en quarantaine sont stockés en toute sécurité dans un format crypté et peuvent être restaurés après l'installation de ESET Cyber Security.

10.3.1 Mise en quarantaine de fichiers

ESET Cyber Security déplace automatiquement les fichiers supprimés en quarantaine (si vous n'avez pas désélectionné cette option dans la fenêtre d'alerte). Vous pouvez mettre manuellement en quarantaine tout fichier suspect en cliquant sur **Quarantaine...** . Il est également possible d'utiliser le menu contextuel : appuyez sur CTRL et cliquez dans le champ vierge, sélectionnez **Quarantaine**, choisissez le fichier à mettre en quarantaine et cliquez sur **Ouvrir**.

10.3.2 Restauration depuis la quarantaine

Les fichiers en quarantaine peuvent également être restaurés à leur emplacement d'origine. Pour ce faire, sélectionnez un fichier en quarantaine, puis cliquez sur **Restaurer**. L'option Restaurer figure également dans le menu contextuel : appuyez sur CTRL et cliquez sur un fichier dans la fenêtre Quarantaine, puis sur **Restaurer**. Le menu contextuel propose également l'option **Restaurer vers...** qui permet de restaurer des fichiers vers un emplacement autre que celui d'origine dont ils ont été supprimés.

10.3.3 Soumission de fichiers de quarantaine

Si vous avez placé en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été considéré infecté par erreur (ex. par l'analyse heuristique du code) et placé en quarantaine, envoyez ce fichier au laboratoire de recherche sur les menaces d'ESET. Pour soumettre un fichier de la quarantaine, appuyez sur CTRL et cliquez sur le fichier, puis sélectionnez l'option **Soumettre le fichier pour analyse** dans le menu contextuel.

10.4 Processus en cours

La liste **Processus en cours** affiche les processus en cours d'exécution sur l'ordinateur. ESET Cyber Security fournit des informations détaillées sur les processus en cours pour protéger les utilisateurs à l'aide de la technologie ESET Live Grid.

- **Processus** : nom du processus en cours d'exécution sur l'ordinateur. Pour afficher tous les processus en cours, il est également possible d'utiliser Activity Monitor (dans */ Applications/Utilities*).
- **Niveau de risque** : dans la majorité des cas, ESET Cyber Security et la technologie ESET Live Grid attribuent des niveaux de risque aux objets (fichiers, processus, etc.) sur la base d'une série de règles heuristiques qui examinent les caractéristiques de chaque objet, puis évaluent le potentiel d'activité malveillante. Cette analyse heuristique attribue aux objets un niveau de risque. Les applications connues marquées en vert sont saines (répertoriées dans la liste blanche) et sont exclues de l'analyse. Cela permet d'accroître la rapidité des analyses à la demande et en temps réel. Une application marquée comme étant inconnue (jaune) n'est pas nécessairement un logiciel malveillant. Il s'agit généralement d'une nouvelle application. Si un fichier vous semble suspect, vous pouvez le soumettre pour analyse au laboratoire de recherche sur les menaces d'ESET. Si le fichier s'avère être une application malveillante, sa signature sera ajoutée à l'une des prochaines mises à jour.
- **Nombre d'utilisateurs** : nombre d'utilisateurs utilisant une application donnée. Ces informations sont collectées par la technologie ESET Live Grid.
- **Temps de découverte** : durée écoulée depuis la détection de l'application par la technologie ESET Live Grid.
- **ID du progiciel** : nom du fournisseur ou du processus de l'application.

Lorsque vous cliquez sur un processus, les informations suivantes apparaissent dans la partie inférieure de la fenêtre :

- **Fichier** : emplacement de l'application sur l'ordinateur.
- **Taille du fichier** : taille physique du fichier sur le disque.
- **Description du fichier** : caractéristiques du fichier basées sur la description émanant du système d'exploitation.
- **ID du progiciel** : nom du fournisseur ou du processus de l'application.
- **Version du fichier** : informations fournies par l'éditeur de l'application.
- **Nom du produit** : nom de l'application et/ou nom de l'entreprise.

10.5 Live Grid

Le système d'alerte anticipée Live Grid veille à ce qu'ESET soit immédiatement et continuellement informé des nouvelles infiltrations. Ce système bidirectionnel remplit un seul objectif : améliorer la protection que nous vous offrons. Pour que nous puissions détecter les nouvelles menaces dès qu'elles apparaissent, nous devons nous mettre en relation avec le plus grand nombre possible de nos clients afin qu'ils agissent en « éclaireurs ». Deux options sont possibles :

1. Vous pouvez choisir de ne pas activer le système d'alerte anticipée Live Grid. Vous ne perdrez aucune fonctionnalité du logiciel et continuerez de recevoir la meilleure protection que nous offrons.
2. Vous pouvez configurer le système d'alerte anticipée Live Grid afin de nous soumettre des informations anonymes sur les nouvelles menaces et l'emplacement du nouveau code menaçant. Ces informations peuvent être envoyées à ESET pour une analyse détaillée. L'étude de ces menaces aidera ESET à mettre à jour sa base de données de menaces et à améliorer la capacité du programme à détecter les menaces.

Le système d'alerte anticipée Live Grid collecte des informations sur votre ordinateur concernant des menaces nouvellement détectées. Ces informations peuvent contenir un exemple ou une copie du fichier dans lequel la menace est apparue, le chemin d'accès à ce fichier, le nom du fichier, la date et l'heure, le processus qui a permis l'apparition de la menace sur votre ordinateur et des informations sur le système d'exploitation de votre ordinateur.

Ce processus peut dévoiler occasionnellement au Laboratoire de menaces ESET certaines informations sur vous ou votre ordinateur (noms d'utilisateur dans un chemin de répertoires, etc.), mais ces informations ne seront utilisées à AUCUNE autre fin que celle de nous permettre de réagir immédiatement aux nouvelles menaces.

Pour accéder à la configuration de Live Grid, cliquez dans le menu principal sur **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd+,*) > **Live Grid**. Sélectionnez l'option **Activer le système d'alerte anticipé Live Grid** pour l'activer, puis cliquez sur l'option **Configuration...** en regard de l'intitulé **Options avancées**.

10.5.1 Configuration de Live Grid

Par défaut, ESET Cyber Security est configuré pour soumettre les fichiers suspects au laboratoire de recherche sur les menaces d'ESET pour obtenir une analyse détaillée. Si vous ne souhaitez pas soumettre ces fichiers automatiquement, désélectionnez l'option **Soumission des fichiers suspects**.

Si vous trouvez un fichier suspect, vous pouvez le soumettre à notre laboratoire de recherche sur les menaces pour analyse. Pour cela, cliquez sur **Outils** > **Soumettre le fichier pour analyse** à partir de la fenêtre du programme principal. S'il s'avère d'une application malveillante, sa signature sera ajoutée à la prochaine mise à jour de la base des signatures de virus.

Soumission des informations statistiques anonymes : le système d'avertissement anticipé ESET Live Grid collecte des informations anonymes sur votre ordinateur concernant des menaces nouvellement détectées. Ces informations incluent le nom de l'infiltration, la date et l'heure de détection, la version du produit de sécurité ESET, ainsi que des informations sur la version du système d'exploitation de votre ordinateur et ses paramètres régionaux. Ces statistiques sont normalement fournies aux serveurs ESET une ou deux fois par jour.

Voici un exemple de statistiques soumises :

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/
rdgFR1463[1].zip
```

Filtre d'exclusion : cette option permet d'exclure certains types de fichier de la soumission. Par exemple, il peut être utile d'exclure des fichiers qui peuvent comporter des informations confidentielles, tels que des documents ou des feuilles de calcul. Les fichiers les plus ordinaires sont exclus par défaut (.doc, .rtf, etc.). Vous pouvez ajouter des types de fichiers à la liste des fichiers exclus.

Email de la personne à contacter (facultatif) : votre adresse électronique est utilisée si l'analyse exige des informations complémentaires. Notez que vous ne recevrez pas de réponse d'ESET, à moins que des informations complémentaires soient nécessaires.

10.6 ESET Social Media Scanner

ESET Social Media Scanner est une application qui vous protège des contenus malveillants distribués par l'intermédiaire des réseaux sociaux. ESET Scanner Réseaux Sociaux surveille les nouveaux contenus des réseaux sociaux (par exemple, les publications sur les murs contenant des liens ou des éléments multimédias) et recherche la présence de code malveillant à l'aide de l'analyse automatique et à la demande. Les résultats de l'analyse sont signalés à l'utilisateur par un message dans l'application proprement dite, dans un message électronique ou dans un commentaire indiquant que l'objet est infecté. Les statistiques hebdomadaires qui sont publiées sur le mur de l'utilisateur indiquent à l'utilisateur qu'il est protégé des menaces.

L'application ESET Social Media scanner est indépendante des autres produits de sécurité ESET et est entièrement gratuite.

Pour accéder à la page Web et télécharger l'application ESET Social Media Scanner, cliquez dans le menu principal d'ESET Cyber Security, sur **Outis** > **ESET Social Media Scanner**.

11. Interface utilisateur

Les options de configuration de l'interface utilisateur permettent d'adapter l'environnement de travail selon vos besoins. Vous pouvez accéder à ces options depuis le menu principal en cliquant sur **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd+,* > **Interface**.

- Pour afficher l'écran d'accueil de ESET Cyber Security au démarrage du système, sélectionnez **Afficher l'écran de démarrage**.
- L'option **Application présente dans le Dock** permet d'afficher l'icône de ESET Cyber Security dans le Dock de Mac OS et de basculer entre ESET Cyber Security et d'autres applications actives en appuyant sur *cmd-tab*. Les modifications entrent en vigueur après le redémarrage de ESET Cyber Security (généralement provoqué par un redémarrage de l'ordinateur).
- L'option **Utiliser le menu standard** permet d'utiliser certains raccourcis clavier (voir Raccourcis clavier 6) et d'afficher des éléments de menu standard (interface utilisateur, Configuration et Outils) sur la barre de menus Mac OS (en haut de l'écran).
- Pour activer les info-bulles de certaines options de ESET Cyber Security, sélectionnez l'option **Afficher les info-bulles**.
- L'option **Afficher les fichiers masqués** permet d'afficher et de sélectionner les fichiers masqués dans la configuration des **cibles à analyser** d'une **analyse de l'ordinateur**.

11.1 Alertes et notifications

La section **Alertes et notifications** vous permet de configurer le mode de traitement des alertes en cas de menace et des notifications système dans ESET Cyber Security.

La désactivation de l'option **Afficher les alertes** désactive les fenêtres d'alerte et n'est recommandée que dans des situations très précises. Nous recommandons à la majorité des utilisateurs de conserver l'option par défaut (activée).

La sélection de l'option **Afficher les notifications sur le Bureau** entraîne l'affichage des fenêtres d'alerte sur le bureau (par défaut dans l'angle supérieur droit de votre écran) sans aucune intervention de l'utilisateur. Vous pouvez définir la période pendant laquelle une notification est affichée en réglant la valeur **Fermer automatiquement les notifications après** X **secondes**.

Pour afficher uniquement les notifications nécessitant une interaction de l'utilisateur lors de l'exécution d'applications en mode plein écran, sélectionnez **Activer le mode plein écran** . Cette option est utile lorsque vous effectuez des présentations, jouez à des jeux ou effectuez toute autre opération nécessitant l'intégralité de l'écran.

11.1.1 Configuration avancée des alertes et notifications

ESET Cyber Security affiche des boîtes d'alerte vous informant de la disponibilité de nouvelles versions du programme, de mises à jour du système d'exploitation, de la désactivation de certains composants du programme, de la suppression de journaux, etc. Vous pouvez éviter l'affichage de chaque notification en sélectionnant l'option **Ne plus afficher cette boîte de dialogue** dans le dialogue correspondant.

Liste des boîtes de dialogue (**Configuration** > **Saisie des préférences de l'application...** > **Alertes et notifications** > **Configuration...**) affiche la liste de toutes les boîtes d'alerte déclenchées par ESET Cyber Security. Pour activer ou masquer chaque notification, cochez la case à gauche du **nom de la boîte de dialogue**. Vous pouvez aussi définir des **conditions d'affichage** des notifications sur les nouvelles versions du programme et du système d'exploitation.

11.2 Privilèges

Les paramètres ESET Cyber Security peuvent être très importants pour la stratégie de sécurité de votre organisation. Des modifications non autorisées peuvent mettre en danger la stabilité et la protection de votre système. Par conséquent, vous pouvez définir les utilisateurs autorisés à modifier la configuration du programme.

Pour définir les utilisateurs privilégiés, cliquez sur **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd+,*) > **Privilèges**.

Il est essentiel que le programme soit correctement configuré pour garantir le maximum de sécurité au système. Tout changement non autorisé peut provoquer la perte de données importantes. Pour définir la liste des utilisateurs privilégiés, sélectionnez les utilisateurs dans la liste **Utilisateurs** dans la partie gauche et cliquez sur **Ajouter**. Pour afficher tous les utilisateurs, sélectionnez **Afficher tous les utilisateurs**. Pour supprimer un utilisateur, sélectionnez son nom dans la liste **Utilisateurs privilégiés** située à droite, puis cliquez sur **Supprimer**.

REMARQUE : si la liste des utilisateurs privilégiés est vide, tous les utilisateurs du système sont autorisés à modifier les paramètres du programme.

11.3 Menu contextuel

Pour activer l'intégration des menus contextuels, cliquez sur **Configuration** > **Saisie des préférences de l'application...** (ou appuyez sur *cmd+,*) > **Menu contextuel** en sélectionnant l'option **Intégrer dans le menu contextuel**. Vous devez vous déconnecter ou redémarrer l'ordinateur pour que les modifications entrent en vigueur. Les options du menu contextuel sont disponibles dans la fenêtre du **Finder** lorsque vous appuyez sur la touche CTRL en cliquant sur n'importe quel fichier.

12. Divers

12.1 Importer et exporter les paramètres

L'importation et l'exportation des configurations de ESET Cyber Security peut être effectuée depuis la section **Setup**.

Ces opérations sont utiles si vous devez sauvegarder votre configuration actuelle de ESET Cyber Security pour l'utiliser ultérieurement. **Exporter les paramètres** est également pratique pour les utilisateurs qui souhaitent utiliser leur configuration préférée de ESET Cyber Security sur plusieurs systèmes. Il est facile d'importer un fichier de configuration afin de transférer les paramètres souhaités.

CYBER SECURITY
ESET Cyber Security vous permet d'enregistrer la configuration en cours dans un fichier et de la restaurer ultérieurement.
Importer et exporter
Importer les paramètres
Exporter les paramètres
Nom de fichier :
Parcourir...
Annuler
OK

12.1.1 Importer les paramètres

Pour importer une configuration, cliquez sur **Configuration** > **Importer et exporter les paramètres...** à partir du menu principal, puis sélectionnez l'option **Importer les paramètres**. Cliquez sur **Parcourir...** pour rechercher le fichier de configuration que vous souhaitez importer.

12.1.2 Exporter les paramètres

Pour exporter une configuration, cliquez sur **Configuration** > **Importer et exporter les paramètres...** à partir du menu principal, puis sélectionnez l'option **Exporter les paramètres**. Utilisez le navigateur pour sélectionner un emplacement de votre ordinateur afin d'enregistrer le fichier de configuration.

12.2 Configuration du serveur proxy

Les paramètres de serveur proxy peuvent être configurés dans **Configuration** > **Saisie des préférences de l'application ...** (ou appuyez sur *cmd+,*) > **Serveur proxy**. La spécification du serveur proxy à ce niveau définit les paramètres de serveur proxy globaux pour toutes les fonctions de ESET Cyber Security. Les paramètres définis ici seront utilisés par tous les modules nécessitant une connexion à Internet. ESET Cyber Security prend en charge les authentifications de type Accès de base et NTLM (NT LAN Manager).

Pour spécifier des paramètres de serveur proxy à ce niveau, cochez la case **Utiliser le serveur proxy**, puis entrez l'adresse IP ou l'URL du serveur proxy dans le champ **Serveur proxy**. Dans le champ **Port**, spécifiez le port sur lequel le serveur proxy accepte les connexions (3128 par défaut).

Si la communication avec le serveur proxy exige une authentification, cochez la case **Le serveur proxy exige une authentification** et entrez un **nom d'utilisateur** et un **mot de passe** valides dans les champs correspondants.

13. Glossaire

13.1 Types d'infiltrations

Une infiltration est un élément de logiciel malveillant qui tente de s'introduire dans l'ordinateur d'un utilisateur et/ou de l'endommager.

13.1.1 Virus

Un virus est une infiltration qui endommage les fichiers existants de votre ordinateur. Les virus informatiques sont comparables aux virus biologiques parce qu'ils utilisent des techniques similaires pour se propager d'un ordinateur à l'autre.

Les virus informatiques attaquent généralement les fichiers, scripts et documents exécutables. Pour proliférer, un virus attache son « corps » à la fin d'un fichier cible. En bref, un virus informatique fonctionne de la manière suivante : après l'exécution du fichier infecté, le virus s'active lui-même (avant l'application originale) et exécute sa tâche prédéfinie. C'est après seulement que l'application originale peut s'exécuter. Un virus ne peut pas infecter un ordinateur à moins qu'un utilisateur n'exécute ou n'ouvre lui-même le logiciel malveillant (accidentellement ou délibérément).

Les virus peuvent varier en fonction de leur gravité et de leur cible. Certains sont extrêmement dangereux parce qu'ils ont la capacité de supprimer délibérément des fichiers du disque dur. D'autres, en revanche, ne causent pas de réels dommages : ils ne servent qu'à gêner l'utilisateur et à démontrer les compétences techniques de leurs auteurs.

Il est important de noter que, contrairement aux chevaux de Troie et aux spyware, les virus sont de plus en plus rares, car d'un point de vue commercial, ils ne sont pas très attrayants pour les auteurs de logiciels malveillants. En outre, le terme « virus » est souvent utilisé mal à propos pour couvrir tout type d'infiltrations. On tend à le remplacer progressivement par le terme « logiciel malveillant » ou « malware » en anglais.

Si votre ordinateur est infecté par un virus, il est nécessaire de restaurer les fichiers infectés à leur état original, en les nettoyant à l'aide d'un programme antivirus.

13.1.2 Vers

Un ver est un programme contenant un code malveillant qui attaque les ordinateurs hôtes et se propage via un réseau. La différence fondamentale entre les virus et les vers est que les vers ont la capacité de se répliquer et de voyager par eux-mêmes. Ils ne dépendent pas des fichiers hôtes (ou des secteurs d'amorçage). Les vers se propagent par l'intermédiaire d'adresses électroniques de votre liste de contacts ou exploitent les vulnérabilités de sécurité des applications réseau.

Les vers sont ainsi susceptibles de vivre beaucoup plus longtemps que les virus. Par le biais d'Internet, ils peuvent se propager à travers le monde en quelques heures seulement et parfois en quelques minutes. Leur capacité à se répliquer indépendamment et rapidement les rend plus dangereux que les autres types de logiciels malveillants.

Un ver activé dans un système peut être à l'origine de plusieurs dérèglements : il peut supprimer des fichiers, dégrader les performances du système ou même désactiver certains programmes. Par sa nature, il peut servir de « moyen de transport » à d'autres types d'infiltrations.

Si votre ordinateur est infecté par un ver, il est recommandé de supprimer les fichiers infectés, car ils contiennent probablement du code malicieux.

13.1.3 Chevaux de Troie

Les chevaux de Troie étaient auparavant définis comme une catégorie d'infiltrations dont la particularité est de se présenter comme des programmes utiles pour duper ensuite les utilisateurs qui acceptent de les exécuter. Aujourd'hui, les chevaux de Troie n'ont plus besoin de se déguiser. Leur unique objectif est de trouver la manière la plus facile de s'infiltrer pour accomplir leurs desseins malveillants. Le terme « cheval de Troie » est donc devenu un terme très général qui décrit toute infiltration qui n'entre pas dans une catégorie spécifique.

La catégorie étant très vaste, elle est souvent divisée en plusieurs sous-catégories :

- Downloader : programme malveillant qui est en mesure de télécharger d'autres infiltrations sur Internet.
- Dropper : type de cheval de Troie conçu pour déposer d'autres types de logiciels malveillants sur des ordinateurs infectés.
- Backdoor : application qui communique à distance avec les pirates et leur permet d'accéder à un système et d'en prendre le contrôle.
- Keylogger : programme qui enregistre chaque touche sur laquelle tape l'utilisateur et envoie les informations aux pirates.
- Composeur : programme destiné à se connecter à des numéros surtaxés. Il est presque impossible qu'un utilisateur remarque qu'une nouvelle connexion a été créée. Les composeurs ne peuvent porter préjudice qu'aux utilisateurs ayant des modems par ligne commutée, qui sont de moins en moins utilisés.

Les chevaux de Troie prennent généralement la forme de fichiers exécutables. Si un fichier est identifié comme cheval de Troie sur votre ordinateur, il est recommandé de le supprimer, car il contient sans doute du code malveillant.

13.1.4 Rootkits

Les rootkits sont des programmes malveillants qui permettent aux attaquants via Internet d'accéder à un système tout en cachant leur présence. Après avoir accédé à un système (généralement en exploitant une vulnérabilité de celui-ci), les rootkits utilisent des fonctions du système d'exploitation pour éviter d'être détectés par les logiciels antivirus : ils cachent leurs processus et fichiers. Il est donc quasiment impossible de les détecter par des techniques de test ordinaires.

13.1.5 Logiciels publicitaires

Le terme anglais « adware » désigne parfois les logiciels soutenus par la publicité. Les programmes qui affichent des publicités entrent donc dans cette catégorie. Les logiciels publicitaires ouvrent généralement une nouvelle fenêtre contextuelle automatiquement dans un navigateur Internet. Cette fenêtre contient de la publicité ou modifie la page

d'accueil du navigateur. Ils sont généralement associés à des programmes gratuits et permettent aux développeurs de ces programmes de couvrir les frais de développement de leurs applications (souvent utiles).

Les logiciels publicitaires proprement dits ne sont pas dangereux ; tout au plus dérangent-ils les utilisateurs en affichant ces publicités. Le danger tient dans le fait qu'ils peuvent aussi avoir des fonctions d'espionnage (comme les spyware).

Si vous décidez d'utiliser un logiciel gratuit, soyez particulièrement attentif au programme d'installation. La plupart des programmes d'installation vous avertissent en effet qu'ils installent également un logiciel publicitaire. Souvent, vous pourrez désactiver cette installation supplémentaire et installer le programme sans logiciel publicitaire.

Certains programmes refusent de s'installer sans leur logiciel publicitaire ou voient leurs fonctionnalités limitées. Cela signifie souvent que les logiciels publicitaires accèdent au système d'une manière « légale », dans la mesure où les utilisateurs l'ont accepté. Dans ce cas, mieux vaut jouer la sécurité. Si un logiciel publicitaire est détecté sur votre ordinateur, il est préférable de le supprimer, car il est fort probable qu'il contienne du code malveillant.

13.1.6 Spyware

Cette catégorie englobe toutes les applications qui envoient des informations confidentielles sans le consentement des utilisateurs et à leur insu. Les spyware utilisent des fonctions de traçage pour envoyer diverses données statistiques telles que la liste des sites Web visités, les adresses électroniques de la liste de contacts de l'utilisateur ou la liste des touches du clavier utilisées.

Les auteurs de ces spyware affirment que ces techniques ont pour but d'en savoir plus sur les besoins et intérêts des utilisateurs afin de mieux cibler les offres publicitaires. Le problème est qu'il n'y a pas de distinction claire entre les applications utiles et les applications malveillantes, et que personne ne peut garantir que les informations récupérées ne sont pas utilisées à des fins frauduleuses. Les données récupérées par les spyware peuvent être des codes de sécurité, des codes secrets, des numéros de compte bancaire, etc. Les spyware sont souvent intégrés aux versions gratuites d'un programme dans le but de générer des gains ou d'inciter à l'achat du logiciel. Les utilisateurs sont souvent informés de la présence d'un spyware au cours de l'installation d'un programme qui vise à les inciter à acquérir la version payante qui en est dépourvue.

Parmi les produits logiciels gratuits bien connus qui contiennent des logiciels espions, on trouve les applications clients de réseaux P2P (poste à poste). Spyfalcon ou Spy Sheriff (et beaucoup d'autres) appartiennent à une sous-catégorie spécifique de logiciels espions : ils semblent être des programmes anti-logiciel espion alors qu'ils sont en réalité eux-mêmes des logiciels espions.

Si un fichier est détecté comme étant un spyware sur votre ordinateur, il est recommandé de le supprimer, car il existe une forte probabilité qu'il contienne du code malveillant.

13.1.7 Applications potentiellement dangereuses

Il existe de nombreux programmes authentiques qui permettent de simplifier l'administration des ordinateurs en réseau. Toutefois, s'ils tombent entre de mauvaises mains, ces programmes sont susceptibles d'être utilisés à des fins malveillantes. ESET Cyber Security permet de détecter ces menaces.

Les applications potentiellement dangereuses sont en général des logiciels commerciaux légitimes. Cette classification comprend les programmes d'accès à distance, les applications de résolution de mot de passe ou les keyloggers (programmes qui enregistrent chaque frappe au clavier de l'utilisateur).

13.1.8 Applications potentiellement indésirables

Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais elles sont susceptibles d'affecter les performances de votre ordinateur. L'installation de ces applications nécessite généralement l'accord de l'utilisateur. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Voici les changements les plus significatifs :

- affichage de nouvelles fenêtres ;
- activation et exécution de processus cachés ;
- augmentation des ressources système utilisées ;
- modification des résultats de recherche ;
- communication des applications avec des serveurs distants.

13.2 Types d'attaques à distance

Les attaquants disposent de nombreuses techniques spéciales pour infiltrer des systèmes à distance. Ces techniques se divisent en plusieurs catégories.

13.2.1 Attaques par déni de service

Le déni de service (DoS) cherche à rendre un ordinateur ou un réseau indisponible pour ses utilisateurs. La communication entre les utilisateurs affectés est bloquée et ne peut plus fonctionner correctement. Les ordinateurs exposés à de telles attaques doivent généralement faire l'objet d'un redémarrage pour fonctionner à nouveau correctement.

Le plus souvent, les cibles sont des serveurs Web et le but est de les rendre indisponibles pendant un certain temps.

13.2.2 Empoisonnement du cache DNS

En empoisonnant le DNS (serveur de noms de domaine), les pirates peuvent faire croire au serveur DNS de n'importe quel ordinateur que les fausses données qu'ils fournissent sont légitimes et authentiques. Ces fausses informations sont mises en cache pendant un certain temps, permettant aux attaquants de réécrire les réponses DNS d'adresses IP. Les utilisateurs qui tentent d'accéder à des sites Web sur Internet téléchargeront alors des virus ou des vers informatiques au lieu du contenu d'origine.

13.2.3 Balayage de ports

Le balayage de ports vise à déterminer quels ports de l'ordinateur sont ouverts sur un ordinateur hôte d'un réseau. Un analyseur de ports est un logiciel conçu pour détecter ces ports.

Un port d'ordinateur est un point virtuel qui traite les données entrantes et sortantes. Il est donc crucial du point de vue de la sécurité. Dans un grand réseau, les informations collectées par les analyseurs de ports peuvent aider à identifier des vulnérabilités potentielles. Cette utilisation est légitime.

Cependant, le balayage des ports est souvent utilisé par des pirates pour tenter de compromettre la sécurité du réseau. La première étape consiste à envoyer des paquets sur chaque port. Selon le type de réponse, il est possible de déterminer quels ports sont utilisés. Le balayage en lui-même est inoffensif, mais sachez que cette opération peut révéler des vulnérabilités potentielles et permettre à des attaquants de prendre le contrôle d'ordinateurs à distance.

Il est recommandé aux administrateurs de réseau de bloquer tous les ports inutilisés et de protéger ceux qui sont utilisés contre tout accès non autorisé.

13.2.4 Désynchronisation TCP

La désynchronisation TCP est une technique utilisée dans les attaques de piratage TCP. Elle est déclenchée par un processus qui associe aux paquets entrants un numéro séquentiel différent du numéro attendu. Ces paquets sont alors rejetés (ou enregistrés en mémoire tampon, s'ils se trouvent dans la fenêtre de communication active).

Dans cette technique, les deux extrémités de la communication rejettent des paquets reçus, ce qui permet aux attaquants de s'infiltrer et de fournir des paquets présentant le numéro séquentiel correct. Les attaquants peuvent même manipuler ou modifier la communication.

Les attaques par piratage TCP visent à interrompre les communications entre serveur et client, ou entre pairs. Elles peuvent souvent être évitées en utilisant une authentification pour chaque segment TCP. Il est également conseillé d'utiliser la configuration recommandée pour vos périphériques réseau.

13.2.5 Relais SMB

SMBRelay et SMBRelay2 sont des programmes spéciaux capables de mener des attaques contre des ordinateurs distants. Ces programmes tirent parti du protocole de partage de fichiers SMB (Server Message Block), qui tourne par dessus NetBIOS. Un utilisateur qui partage un dossier ou un répertoire sur un LAN utilise fort probablement ce protocole de partage de fichiers.

Au sein d'une communication en réseau local, les ordinateurs s'échangent des hachages de mots de passe.

SMBRelay reçoit une connexion sur les ports UDP 139 et 445, relaie les paquets échangés entre le client et le serveur, puis les modifie. Après la connexion et l'authentification, le client est déconnecté. SMBRelay crée alors une nouvelle adresse IP virtuelle. SMBRelay relaie les communications du protocole SMB à l'exception de la négociation et de l'authentification.

Les attaquants à distance peuvent utiliser l'adresse IP tant que l'ordinateur client est connecté.

SMBRelay2 fonctionne selon le même principe que SMBRelay, si ce n'est qu'il utilise des noms NetBIOS plutôt que des adresses IP. Les deux programmes peuvent mener des attaques de type « man-in-the-middle ». Ces attaques permettent à leurs auteurs de lire, insérer et modifier les messages échangés entre deux points de communication à leur insu. Les ordinateurs exposés à de telles attaques s'arrêtent souvent de répondre ou redémarrent de manière inattendue.

Pour éviter ces attaques, nous recommandons d'utiliser des mots de passe ou des clés d'authentification.

13.2.6 Attaques par ICMP

ICMP (Internet Control Message Protocol) est un protocole Internet populaire et largement utilisé. Il est essentiellement utilisé par des ordinateurs en réseau pour envoyer divers messages d'erreur.

Les attaquants à distance tentent d'exploiter les faiblesses du protocole ICMP. Celui-ci est conçu pour une communication unidirectionnelle ne nécessitant aucune authentification. Cela permet aux attaquants de déclencher des attaques par déni de service ou d'autres attaques permettant à des utilisateurs non autorisés d'accéder aux paquets entrants et sortants.

Exemples types d'attaques ICMP : envoi massif de pings ou de messages ICMP_ECHO et attaques par rebond. Les ordinateurs exposés à une attaque ICMP sont sensiblement ralentis (pour toutes les applications utilisant Internet) et éprouvent de la difficulté à se connecter à Internet.

13.3 Courrier électronique

Le courrier électronique (e-mail) est une forme de communication moderne qui présente de nombreux avantages. Elle est souple, rapide et directe, et a joué un rôle crucial dans la prolifération d'Internet dans le début des années 1990.

Malheureusement, le large anonymat que permettent le courrier électronique et Internet laisse une voie ouverte à des activités illégales telles que le spam. Celui-ci couvre aussi bien des publicités non sollicitées que des canulars et la diffusion de logiciels malveillants. L'inconfort et le risque que cela représente pour vous sont aggravés par le fait que le coût d'envoi des spams est infime et que leurs auteurs disposent de nombreux outils pour se procurer des nouvelles adresses électroniques. Qui plus est, le volume et la diversité du spam rendent difficile sa régulation. Plus longtemps vous utilisez la même adresse électronique, plus elle risque d'aboutir dans la base de données d'un moteur de spam. Voici quelques conseils de prévention :

- Si possible, ne publiez pas votre adresse électronique sur Internet,
- ne donnez votre adresse électronique qu'à des personnes de confiance,
- dans la mesure du possible, n'utilisez pas d'alias courants ; plus votre alias est compliqué, plus il sera difficile à épier,
- ne répondez pas à des messages de spam déjà parvenus dans votre boîte de réception,

- soyez prudent lorsque vous complétez des formulaires sur Internet ; méfiez-vous en particulier d'options telles *Oui, je souhaite recevoir des informations*,
- utilisez des adresses électroniques « spécialisées » - par exemple une pour le travail, une pour vos amis, etc.,
- changez d'adresse électronique de temps à autre,
- utilisez une solution antispam.

13.3.1 Publicités

La publicité sur Internet est une des formes de communication commerciale en plus forte croissance. Ses principaux avantages en termes de marketing sont ses coûts minimes et une communication très directe ; qui plus est, les messages sont diffusés quasi instantanément. Nombre d'entreprises recourent à des outils de marketing par courrier électronique pour s'assurer une communication efficace avec leurs clients et leurs prospects.

Ce type de publicité est légitime, car il peut être intéressant de recevoir des informations commerciales sur certains produits. Hélas, de nombreuses entreprises envoient des messages commerciaux non sollicités en masse. Elles franchissent alors la frontière entre la publicité par courrier électronique et le spam.

Le volume de messages non sollicités est devenu un réel problème et ne montre aucun signe de ralentissement. Leurs auteurs tentent souvent de cacher le spam sous les dehors de messages légitimes.

13.3.2 Canulars

Un canular est une information erronée diffusée sur Internet. Le courrier électronique et les outils de communication tels que Skype et ICQ en sont les vecteurs privilégiés. Le message en lui-même est souvent une plaisanterie ou une légende urbaine.

Les canulars relatifs à des virus informatiques visent à susciter la crainte, l'incertitude et le doute chez les destinataires, en tentant de leur faire croire qu'il existe un « virus indétectable » qui supprime des fichiers et récupère les mots de passe ou effectue d'autres opérations néfastes sur leur système.

Certains canulars opèrent par contagion, en poussant leurs destinataires à transférer le message à leurs contacts. Il existe des canulars sur les téléphones mobiles, des faux appels à l'aide, des prétendus transferts de fonds secrets venant de l'étranger, etc. Souvent, il est malaisé de déterminer l'intention de l'auteur du message.

Si vous recevez un message vous invitant à le transférer à tous vos contacts, il est bien possible qu'il s'agisse d'un canular. De nombreux sites sur Internet permettent d'en vérifier la légitimité. Avant de transférer un tel message, effectuez une recherche sur Internet pour vous assurer qu'il ne s'agit pas d'un canular.

13.3.3 Hameçonnage

Le hameçonnage (en anglais : phishing) définit une activité criminelle basée sur l'ingénierie sociale (consistant à manipuler des personnes pour leur soutirer des informations confidentielles). Son but est d'obtenir l'accès à des données sensibles telles que des numéros de compte bancaire, des codes PIN, etc.

Souvent, la technique consiste à se faire passer pour une personne ou une entreprise de confiance (p. ex. une institution financière, une société d'assurances). Le message électronique peut sembler authentique et contiendra des graphismes et du contenu pouvant provenir à l'origine de la source usurpée. Sous divers prétextes (vérification des données, opérations financières), vous serez invité à fournir certaines données personnelles telles qu'un numéro de compte bancaire ou un nom d'utilisateur et un mot de passe. Ces données, si vous les envoyez, pourront facilement être détournées et utilisées à mauvais escient.

Les banques, compagnies d'assurances et autres entreprises légitimes ne vous demanderont jamais des noms d'utilisateur et des mots de passe par le biais de messages non sollicités.

13.3.4 Identification du spam

D'une manière générale, plusieurs signes peuvent vous aider à identifier du spam (messages non sollicités) dans votre boîte aux lettres. Si un message répond au moins à quelques-uns des critères ci-dessous, ce sera probablement un spam.

- L'adresse de l'expéditeur n'appartient pas à un de vos contacts,
- on vous propose une somme d'argent importante, mais vous devez commencer par engager un petit montant,
- sous divers prétextes (vérification des données, opérations financières), vous serez invité à fournir certaines données personnelles telles qu'un numéro de compte bancaire ou un nom d'utilisateur et un mot de passe,
- le message est rédigé dans une langue étrangère,
- vous êtes invité à acheter un produit qui ne vous intéresse pas ; si vous décidez de l'acheter quand même, assurez-vous que l'expéditeur est un vendeur fiable (consultez le fabricant original du produit),
- certains mots sont mal orthographiés afin de contourner les filtres antispam (par exemple *vaigra* au lieu de *viagra*, etc.).